1/2007

Datenschutz Nachrichten

30. Jahrgang
ISSN 0137-7767
9,00 Euro

Reise und Touristik

Gefährliche TouristInnen ■ Welt der Reise-Informationen ■ Datenschutz bei Kreuzfahrten ■ Datenschutztipps für Urlaubsreisende ■ Tagung »Die neue Überwachung« ■ Personenkennzeichen im Sport ■ Nachrichten ■ Technik ■ Gentechnik ■ Rechtsprechung ■ Buchbesprechungen ■ Presseerklärungen

Deutsche Vereinigung für Datenschutz e.V.
www.datenschutzverein.de

Termine

15.07.2007
BigBrotherAwards 2007 Nominierungsschluss
www.bigbrotherawards.de

22.07.2007
DVD-Vorstandssitzung in Frankfurt*

01.08.2006
Redaktionsschluss DANA 3/2007
Sozialdatenschutz

27.08.2006
Sommerakademie 2007:
Offene Kommunikationsgesellschaft und Terrorbekämpfung – ein Widerspruch?
Kiel, Hotel Maritim
www.datenschutzzentrum.de/sommerakademie/

30.09.2007
DVD-Vorstandssitzung in Bonn*

11.10.2007, 18:00 Uhr
DVD-Mitgliederversammlung in Bielefeld
Ravensberger Spinnerei, Raum 240,
Ravensberger Park 1, 33607 Bielefeld

12.10.2006, 10:00 Uhr
30 Jahre DVD – ein Grund zum Feiern
anschließend
BigBrotherAwards 2007 Verleihung
Bielefeld

* interessierte DVD-Mitglieder können gerne teilnehmen, bitte in der Geschäftsstelle melden

Autoren dieser Ausgabe

Hans-Jürgen Burger

Berater für Datenschutz und IT-Sicherheit, Leipheim
Mitglied des Vorstandes der DVD
hans-juergen.burger@datenschutzbuero.net

Heiner Busch

Redakteur von Bürgerrechte & Polizei/CILIP und Vorstandsmitglied des Komitees für Grundrechte und Demokratie,
heinerbusch@freesurf.ch

Sönke Hilbrans

Rechtsanwalt, Berlin
Vorsitzender der Deutschen Vereinigung für Datenschutz
hilbrans@diefirma.net

Dr. Leon Hempel

Sozialwissenschaftler am Zentrum Technik und Gesellschaft der Technischen Universität Berlin und Dozent am Masterstudiengang Historische Urbanistik.
Internationale Projekte zu Themen der Überwachung, insbesondere zu sozialen und politischen Aspekten. Für Transport for London untersuchte er sehr umfangreiche Systeme hinsichtlich Abschreckung und Lernverhalten. Initiator der Konferenz »The New Surveillance«.

Dr. Thilo Weichert

Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, Kiel
weichert@datenschutzzentrum.de

Donnerstag, 11.10.2007, 18 Uhr

Mitgliederversammlung der DVD
in Bielefeld

Freitag, 12.10.2007, 10 – 17 Uhr

30 Jahre DVD – ein Grund zum Feiern

Jubiläumsveranstaltung + Datenschutztag aus Anlaß des 30jährigen Bestehens der Deutschen Vereinigung für Datenschutz
unter Beteiligung von
Wolfgang Däubler • Reinhard Frenkel
Burkhard Hirsch • Peter Schaar
Bettina Sokohl • Johann Bizer (angefr.)
Sie können sich vormerken lassen unter:
tagung2007@datenschutzverein.de

Freitag, 12.10.2007, 18 Uhr

Verleihung der BigBrotherAwards 2007

Die Veranstaltungen finden statt in der Ravensberger Spinnerei,
Ravensberger Park 1, 33607 Bielefeld

DANA
Datenschutz Nachrichten
ISSN 0137-7767
30. Jahrgang, Heft 1

Herausgeber
Deutsche Vereinigung für Datenschutz e.V. (DVD)
DVD-Geschäftsstelle:
Bonner Talweg 33-35, 53113 Bonn
Tel. 0228-222498
E-Mail: dvd@datenschutzverein.de
www.datenschutzverein.de

Redaktion (ViSdP)
Sönke Hilbrans, Karin Schuler
c/o Deutsche Vereinigung für Datenschutz e.V. (DVD)
Bonner Talweg 33-35, 53113 Bonn
dana@datenschutzverein.de
Den Inhalt namentlich gekennzeichneter Artikel verantworten die jeweiligen Autoren.

Druck
Wienands Printmedien GmbH
Linzer Str. 140, 53604 Bad Honnef
wienandsprintmedien@t-online.de
Tel. 02224 989878-0
Fax 02224 989878-8

Bezugspreis
Einzelheft 9 Euro. Jahresabonnement 32 Euro (incl. Porto) für vier Hefte im Jahr. Für DVD-Mitglieder ist der Bezug kostenlos.
Ältere Ausgaben der DANA können teilweise noch in der Geschäftsstelle der DVD bestellt werden.

Leserbriefe
Leserbriefe sind erwünscht, deren Publikation sowie eventuelle Kürzungen bleiben vorbehalten.

Abbildungen
Titelbild: Frans Jozef Valenta
Rückseite: Sabine Steinort

Urlaub

Wer eine Reise tut, der kann was erzählen, so hieß es früher. Heute ist es ein wenig anders: Wer eine Reise tun will, der muss einiges über sich erzählen. Und er oder sie wird nicht wissen, wer es erfährt. Sicher ist nur: so schnell wird nicht in Vergessenheit geraten, was preisgegeben wurde. Dazu erzählen noch andere etwas über unsere Reisen: wo wir gewesen sind, was wir dort gemacht haben, was wir gegessen und wie viel Geld wir sonst noch wofür ausgegeben haben.
Weltumspannende Buchungssysteme erfassen die Rahmendaten unserer Reisen, wann womit wohin. Unsere maschinenlesbare Ausweise werden gescannt, demnächst womöglich per Funk, ohne dass wir es merken. Intelligente Kameras überwachen jeden Schritt am Flughafen. Fahren wir mit dem Auto, verfolgen die Pkw-Kennzeichenscanner unseren Weg. Touristenausweise am Reiseort registrieren jeden Besuch einer Sehenswürdigkeit, jede Nutzung der Infrastruktur. Mit dem Skipass wird festgehalten, wann wir mit welchem Lift gefahren und wie lange wir für die Abfahrt gebraucht haben.
Was mit den Daten passiert, werden wir nicht erfahren. Solange wir nicht die falschen Länder bereist und auch noch die falschen Bücher gekauft haben, werden wir wahrscheinlich nicht gleich auf einer Terrorliste oder in irgendeinem Land im Gefängnis landen. Wie unsere Reisen unser Kreditrating beeinflussen, merken wir nicht.

Rainer Scholl

Inhalt

Termine, Autoren 2
Editorial, Impressum, Inhalt 3

Touristik
Heiner Busch
Gefährliche TouristInnen 4
Hans-Jürgen Burger
Die Welt der Reise-Informationen 6
Oskar
Kreuzfahrten: Nichts für Datenschutzbewusste 10
Thilo Weichert
ULD-Datenschutz-Tipps für Urlaubsreisende 11
Leon Hempel
Die Neue Überwachung – internationale Experten diskutieren eine adäquate Bewertung 13
Thilo Weichert
Weshalb das Personenkennzeichen in der Sportsicherheit unerlässlich ist 16
Stellungsnahme der DVD zur geplanten Änderung des Passgesetzes 18

Datenschutznachrichten
Tourismus 20
Deutsche Datenschutznachrichten 21
Ausländische Datenschutznachrichten 29
Technik-Nachrichten 35
Gentechnik-Nachrichten 36

Rechtsprechung 37
Buchbesprechungen 41

Pressemitteilungen
Einhellige Ablehnung der Koalitionspläne zur Vorratsdatenspeicherung 43
10.000 wollen gegen Abbildung ihrer Kommunikation nach Karlsruhe ziehen 44
Gegen Bürokratie und Staatswillkür 45
Privatsphäre muss vor heimlichen Online-Durchsuchungen geschützt bleiben 45
Schäubles Daten-Exhibitionismus gefährdet die Sicherheit 46
Marke »Made in Germany« durch Pläne des Innenministeriums beschädigt 47
Freiheit statt Angst – Demo gegen Sicherheits- und Überwachungswahn 48
EG-Kommission fürchtet um Richtlinie zur Vorratsdatenspeicherung 49
Fast 2000 Menschen demonstrieren in Frankfurt für »Freiheit statt Angst« 50
Kampagne »SPD, CDU, CSU gegen Vorratsdatenspeicherung« 50
RFID-Schutzhüllen 50

Jahresregister 2006 Innenteil

Heiner Busch

Gefährliche TouristInnen

Biometrische Kontrolle und geheimdienstliche Überwachung

Die EU und ihre Mitgliedstaaten befürchten, TouristInnen aus armen Ländern könnten sich in illegale ImmigrantInnen verwandeln oder – schlimmer noch – kriminelle oder terroristische Ziele verfolgen. Mit dem geplanten Visa-Informationssystem (VIS) und dem Schengener Informationssystem der zweiten Generation (SIS II) erwartet Nicht-EU-BürgerInnen nun die biometrische Kontrolle.

Mit Hochdruck arbeitet die EU derzeit am Aufbau und den rechtlichen Grundlagen der beiden neuen Datensysteme. Die grundlegenden Rechtsakte über das SIS II, das voraussichtlich 2009 ans Netz gehen und eine technische Interimslösung (»SISone4all«) ablösen wird, sind bereits verabschiedet.[1] Das Europäische Parlament hatte im Oktober 2006 einem zuvor hinter verschlossenen Türen mit dem Ministerrat ausgedealten »Kompromiss« zugestimmt.[2] Nachdem das Parlament beim SIS II eingeknickt ist, wird es beim VIS kaum Widerstand leisten.

Die beiden neuen Systeme, die auf einer gemeinsamen technischen Plattform betrieben werden, unterstreichen den engen Zusammenhang zwischen der quasi-polizeilichen Ausländer- und Visumspolitik der EU einerseits und der in starkem Maße auf AusländerInnen ausgerichteten Polizeikooperation. So werden einerseits die Konsulate das polizeiliche SIS II abrufen können, während andererseits die Polizei Zugang zum VIS erhält. Sowohl die Personendatensätze des SIS II als auch das VIS werden biometrische Daten – Fingerabdrücke und digitalisierte Fotos – enthalten.

Biometrische Erfassung im Konsulat

Schon das bisherige SIS war mehr als das »Fahndungssystem«, als das es in der Öffentlichkeit verkauft wurde. Seit seiner Inbetriebnahme im März 1995 beziehen sich regelmäßig weit über 80 Prozent der im SIS gespeicherten Personendaten auf Nicht-EU-BürgerInnen, denen überwiegend aus rein ausländerrechtlichen Gründen die Einreise verweigert werden sollte.[3] Zu diesen Daten haben auch die Konsulate der Schengen-Staaten Zugriff.

In Zukunft werden die Konsulate nicht mehr nur prüfen, ob eine Person zur Einreise- bzw. Visumsverweigerung im SIS ausgeschrieben ist, sondern gleich alle, die ein Visum für die EU wollen, im VIS erfassen – und zwar unabhängig davon, ob sie das Visum auch erhalten.[4] Bei 20 Millionen Anträgen pro Jahr und einer Speicherungsfrist von fünf Jahren werden im VIS dereinst 100 Millionen Nicht-EU-BürgerInnen erfasst sein.

Das VIS soll zum einen alphanumerische Daten enthalten: die Personalien der Visums-AntragstellerIn, Art und Nummer des Reisedokuments, gegebenenfalls Angaben zur einladenden Person oder zum einladenden Unternehmen, Angaben zu früheren Anträgen einschließlich ihrer Bewilligung, Ablehnung, Verlängerung etc. und der Gründe dafür sowie den »Status« der Bearbeitung durch die Konsulate und nationalen »Visumsbehörden« und schließlich die Nummer der in den Pass einzuklebenden Visumsmarke. Biometrische Daten – digitalisierte Fotos und Fingerabdrücke – sollen zudem sicherstellen, dass niemand mit falschen Papieren einer Visumsverweigerung zu entgehen versucht.

Namen sind Schall und Rauch

Verändern wird sich auch die Grenzkontrolle. Diese besteht bisher mindestens in einer Kontrolle der Papiere, d.h. des Passes und des darin eingeklebten maschinenlesbaren Visumsstickers, und in einer Abfrage der Personalien im SIS. Mit der Einführung der beiden neuen Datensysteme wird diese Kontrolle »biometrisiert«.

Laut Artikel 22 der SIS II-Verordnung sollen die hier gespeicherten biometrischen Daten nur zur »Bestätigung der Identität eines Drittstaatsangehörigen« herangezogen werden, wenn vorher die Abfrage nach den »alphanumerischen Daten« zu einem »Treffer« geführt hat. Gleich im nächsten Satz heißt es jedoch: »Sobald technisch möglich« – und das wird bereits kurz nach Inbetriebnahme des Systems der Fall sein – »können Fingerabdrücke auch herangezogen werden, um Drittstaatsangehörige auf der Grundlage ihres biometrischen Identifikators zu identifizieren.« Das Scannen der Fingerabdrücke, die schnelle Form der erkennungsdienstlichen Behandlung, wird damit die Überprüfung der Personalien ersetzen – und zwar sowohl bei der Grenzkontrolle als auch bei den zunehmenden Kontrollen im Inland.

Kontrollieren werden die PolizistInnen aber nicht nur mit dem SIS II, sondern auch mit dem VIS. Das EP hatte ursprünglich vertreten, dass eine VIS-Abfrage zunächst nur anhand der Personalien und der Nummer des Visumsaufklebers erfolgen sollte. Nach dem SIS II-»Kompromiss« dürfte diese Position hinfällig sein.

Schon Ende 2005 hatte die EU-Kommission in ihrer Mitteilung »über die Verbesserung der Effizienz der europäischen Datenbanken« erklärt, dass die Abfrage von alphanumerischen Daten in einer Datenbank von der Größe des VIS zu »langen Auflistungen von Treffern« führen würde, die dann »in einem arbeitsaufwändigen Verfahren einzeln überprüft werden müssen, was im

---

1 Amtsblatt der EU L 381 v. 28.12.2006.

2 EP: A6-0353/2006, A6-0354/2006 und A6-0355/2006 v. 25.10.2006.

3 Zahlen zum Datenbestand und zu den Hits für Jahresbeginn 2006, Bundestagsdrucksache 16/1044 v. 24.3.2006 und – mit Interpretation in: Bürgerrechte & Polizei/CILIP 84 (2/2006), S. 30-33.

4 Ratsdokument 5213/07 v. 11.1.2007 (nur zugänglich auf www.statewatch.org/news) enthält den ursprünglichen Vorschlag der Kommission zur VIS-Verordnung und die neueste Version des Rates.

Rahmen von Grenzkontrollen oft nicht zu leisten ist.« Die Abfrage von biometrischen Merkmalen ermögliche dagegen »ein bisher nicht gekanntes Maß an Präzision.«[5] Nach der derzeit letzten Version des Ministerrates von Anfang Januar 2007 soll das VIS bei Grenzkontrollen und bei Kontrollen im Inland nach der Nummer des Visumsaufklebers und nach den Fingerabdrücken abgefragt werden. Auf das Scannen der Fingerabdrücke will der Rat nur verzichten, wenn das Verkehrsaufkommen an Land- oder Seegrenzen zu hoch ist. Wird eine Person hingegen der illegalen Einreise oder des illegalen Aufenthalts verdächtigt, sollen die PolizistInnen nur noch nach den Fingerabdrücken abfragen.[6]

Schlapphüte mit dabei

Dass die (Grenz-)Kontrolle nicht der einzige polizeiliche Zweck sein würde, dem die beiden neuen Systeme dienen sollen, war seit langem klar. Für das SIS (II) hatte der Rat bereits im Jahre 2003 den Zugang von Europol und Eurojust beschlossen. Er konnte das damals noch im Alleingang – ohne das Parlament. Im letzten Jahr hat er vorerst auf den Zugang der nationalen »Behörden der Inneren Sicherheit« verzichtet. Bereits Anfang Dezember kündigte die damals finnische Ratspräsidentschaft jedoch an, dass in dieser Frage ein zusätzlicher Rechtsakt notwendig sei – ein Beschluss, zu dem der Rat das Parlament dann nicht mehr braucht.[7]

Für das VIS gibt es bereits seit November 2005 einen entsprechenden Entwurf, der sowohl Europol als auch den nationalen Sicherheitsbehörden einen Datenzugang eröffnen soll. Nach dem ursprünglichen Vorschlag der Kommission soll dieser Zugriff jeweils über eine »zentrale Zugangsstelle« pro Mitgliedstaat und bei Europol erfolgen. In jedem Einzelfall hätte die betreffende Behörde begründen sollen, dass die Daten für die »Prävention, Aufdeckung und Untersuchung terroristischer oder sonstiger schwerwiegender Straftaten erforderlich« seien.

Anfängliche Bedenken, dass sich damit auch die Geheimdienste an VIS-Daten bedienen könnten,[8] hat die Polizeiarbeitsgruppe des Rates schnell fallen lassen. In ihrem vorläufigen Beratungsergebnis von Anfang August 2006[9] forderte die Ratsarbeitsgruppe, dass jeder Mitgliedstaat die zugriffsberechtigten Behörden selbst bestimmen sollte. Von Anträgen und Begründungen im Einzelfall will der Rat nichts wissen. Er propagiert stattdessen einen »schnellen und praktikablen«, direkten Zugang auch der Dienste zum VIS.

Diesen Ansinnen wird die Kommission wohl kaum etwas entgegensetzen. In ihrer bereits zitierten Mitteilung über die Effizienz der EU-Datensysteme forderte sie den Zugang der für die Bekämpfung von Kriminalität und Terrorismus zuständigen Behörden zum VIS, zum SIS II und zu Eurodac, dem Datensystem für Fingerabdrücke von Asylsuchenden. Darüber hinaus möchte sie ein Aus- und Einreise-Erfassungssystem und schließlich ein europäisches Passregister, das die bessere Identifizierung auch der EU-BürgerInnen ermöglichen sollte.[10] Spätestens dann rückt die biometrische Kontrolle, die jetzt für Drittstaatsangehörige ansteht, auch für die BürgerInnen der Mitgliedstaaten in greifbare Nähe.

5 Kom (2005) 597 endg. v. 24.11.2005.

6 S. die Art. 16 ff in der Ratsversion des Verordnungsentwurfs, Ratsdokument 5213/07 a.a.O. (Fn. 4).

7 KOM (2005) 600 endg. v. 24.11.2005.

8 Ratsdokument 9199/06 v. 11.5.2006.

9 Ratsdokument 11405/06 v. 3.8.2006.

10 Kom (2005) 597endg. v. 24.11.2005.

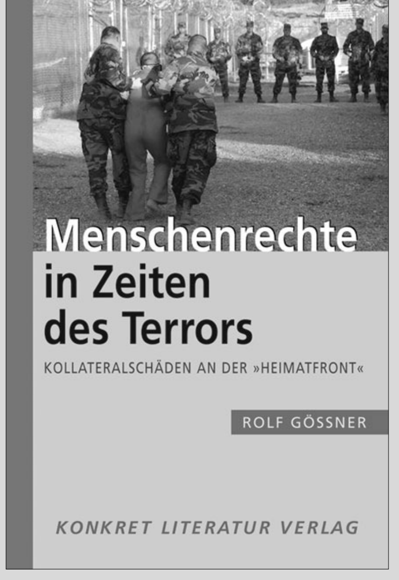
Rolf Gössner: Menschenrechte in Zeiten des Terrors – Kollateralschäden an der »Heimatfront«

So viel Gössner war noch nie: der Geheimdienstkritiker referiert auf 245 dicht beschriebenen Seiten die Folgen des September 2001 für die Bürgerrechte in Deutschland. Die Folgen, um die es Gössner geht, sind hausgemacht, denn nicht der Terrorismus, sondern eine exzessive Anti-Terrorpolitik stehen im Zentrum seiner Betrachtungen.

Wie er eingangs richtig bemerkt, ist dem Publikum angesichts der Masse von Anti-Terror-Maßnahmen seit 2001 der Überblick längst abhanden gekommen. Hier will Gössner nachhelfen, und er tut es kompakt und prägnant. Der Autor kennt sie alle: Die Protagonisten, ihre Argumente und seziert die Folgen.

Wer sich in den letzten sechs Jahren kein umfassendes Zeitungsarchiv angelegt hat, um die Politik der inneren Sicherheit in Deutschland noch zu überschauen, wird mit Rolf Gössners Bilderbogen die entscheidenden Maßnahmen ebenso zur Hand haben wie die Grundzüge der bürgerrechtlichen Kritik. Ein Stichwortverzeichnis erleichtert die Orientierung.

Gössners eigener Standpunkt ist nach wenigen Seiten klar, aber der Autor hält sich selbst mit einer Analyse des großen Ganzen weitgehend zurück. Seine knappen und in der bekannten Art zugespitzten politischen Analysen lassen die kritischen Stimmen der letzten Jahre erneut zu Wort kommen, ein who is who der Verteidiger des liberalen Rechtsstaates von Gerhard Baum bis Thilo Weichert. Dazu benennt er an vielen Stellen die maßgeblichen (und den LeserInnen der DANA gut bekannten) bürgerrechtlichen Initiativen. Ein gut lesbares Handbuch der so genannten inneren Sicherheit.



Konkret Literatur Verlag, Hamburg 2007
ISBN 978-3-89458-252-4, 17 €
www.konkret-literatur-verlag.de
info@konkret-literatur-verlag.de

Hans-Jürgen Burger

Die Welt der Reise-Informationen

Bevor wir uns in den wohlverdienten Urlaub begeben, haben unsere Daten bereits eine weite Reise hinter sich. Durch die Erfassung im Reisebüro oder durch unsere eigene Onlineeingabe befinden sich unsere Daten in Systemen, über die wir keinerlei oder nur sehr geringe Informationen haben. Wir vertrauen diesen Systemen und den Menschen, die unsere Daten verarbeiten, meist blind. Gemäß dem Motto eines Anbieters[1] für sein Produkt »Verkaufen Sie die ganze Welt des Reisens« geht die Reisebranche auf Datenfang und stellt all ihre erhobenen Informationen an einer Vielzahl von Schnittstellen zu Verfügung.

Die heimliche Macht der elektronischen Buchungssysteme

Inzwischen lassen sich die ausgefallensten Reisewünsche erfüllen: von Alaska bis Zypern und von der Antilopen- bis zur Walbesichtigung ist heutzutage alles zu buchen. Die Wege, über die Reisewillige mit einem Reiseveranstalter oder einer Fluglinie in Kontakt treten können, sind vielfältig; das gefällt dem Buchenden. Dank Internet und Reisebörsen sowie einschlägig bekannten Veranstaltern mit Reisebüros findet sich bestimmt das richtige Reiseziel. Zur Ergänzung kann man sich auch in bekannten Reiseforen sachkundig machen. Oft meint man, ein Schnäppchen gefunden zu haben, doch genauso oft irrt man auch.

Die Reisebranche gerät durch die Billiganbieter immer mehr unter Druck. Sie »häutet sich«, wie es der TUI-Vorstandschef Michael Frenzel anlässlich des FVW-Tourismuskongresses[2] in Düsseldorf bezeichnete.

Die Reisebrache ist in der Zwischenzeit weltweit vernetzt und die beiden Produkte,[3] mit denen die Transaktionen mehrheitlich ausgeführt werden, haben genügend Informationen, um Nachrichtendienste weltweit mit den gewünschten Informationen über eine bestimmte Zielgruppe oder Person zu versorgen.

Der Anbieter Amadeus preist seinen Kunden (mehrheitlich Reisebüros und Fluggesellschaften) seine Sales & E-Commerce (Vista Selling) Plattform mit folgenden Worten an:

»Willkommen bei der Amadeus Selling Platform, der ersten voll integrierten browserbasierten Vertriebsplattform, durch die wir Ihnen noch mehr Möglichkeiten bieten, Ihren Kunden die ganze Welt des Reisens zu verkaufen. Nicht nur die Pauschalreise oder das Flugticket, sondern auch den Mietwagen, das Hotel und viele Serviceleistungen mehr. Mit der Amadeus Selling Platform können Sie Ihre Kompetenzen voll ausspielen.«

Diese Aussage verheißt nichts Gutes für den Datenschutz. Die Vernetzung, von der der Reisende in der Regel nichts erfährt, ist erschreckend; insbesondere, wenn man bedenkt, dass Amadeus sich bereits bei über 150 Fluggesellschaften[4] weltweit im Einsatz befindet. Dazu kommen noch Reisebüros, Hotels, Autovermietungen, Bahn, Fähren und Versicherungsgesellschaften, die ebenfalls mit dem System[5] arbeiten. Amadeus ist rund um die Uhr online, 24 Stunden pro Tag, 7 Tage pro Woche und an 365 Tagen im Jahr. Das ermöglicht permanente Kommunikation und Verfügbarkeit aller im System vorhandenen Informationen, die nicht mehr aus unterschiedlichen Quellen zusammengetragen werden müssen. Die Verknüpfung der Daten ist jederzeit möglich und das ohne das Wissen der Reisenden. Dank dieses ausgeklügelten Systems kann der Reisebüromitarbeiter oder die nette Dame am Schalter einer Fluglinie auf Knopfdruck sämtliche über eine Person vorhandenen Informationen abrufen. Amadeus hat sich in den letzten Jahren zu einem universellen Datenpool personenbezogener Daten gemausert. Ähnlich wie beim Paketdienst kann der Reisende Buchungsstatus und alle Details[6] seiner Reise per Internet rund um die Uhr abrufen. Der Mensch als Päckchen oder Reisetracking als Zukunftsvision?

»Wer gelangt noch alles an diese Informationen?« ist die Frage, die wir uns stellen sollten. Dass die Passagierdatenweitergabe an die USA zur Normalität geworden ist und Vielflieger sich darüber nicht mehr erzürnen, ist schlimm genug. Doch welche Notwendigkeit zur Datenweitergabe besteht bei Reisenden, die ein Hotel buchen? Da gewinnt die Aussage des Anbieters »Öffnen Sie die Tür & sehen Sie Mehr ...« eine ganz neue Bedeutung. Natürlich ist es für den Reisebüromitarbeiter eine Erleichterung, wenn er über alle Informationen,[7] die der Kunde gerne hätte, exakte Auskunft geben kann. Die Schmerzgrenze wird allerdings spätestens dann überschritten, wenn Kundeninformationen ins Netz gelangen, wie folgendes Beispiel[8] aus den Erfahrungsberichten von Amadeus zeigt:

«Kleinigkeiten, die das Ganze ausmachen

In der Nachbarschaft hat ein Unternehmensberater sein Büro, der viel unterwegs ist. Vornehmlich Osteuropa: Warschau, Budapest, Sofia. Der Mann hat wenig Zeit aber jedes mal die gleichen anspruchsvollen Wünsche: Business Class Flug, gutes Hotel mit Spa, aber nicht zu teuer, Nichtraucherzimmer und einiges mehr. Wir sind inzwischen ein eingespieltes Team. Er kommt kurz rein oder ruft an, nennt mir Ort und Reisedaten und ist wieder

---

1 www.amadeus.com.

2 http://www.handelsblatt-topix.com/news/Unternehmen/Handel-Dienstleistungen/_pv/_p/200040/_t/ft/_b/1137569/default.aspx/tui-chef-erwartet-radikalen-wandel-in-der-reisebranche.html.

3 www.amadeus.com, www.worlsspan.com

4 z.B. Air Canada, Air France, bmi, Croatia Airlines, Finnair, Iberia, Iclandair, Luxair, Lufthansa, Quantas, Varig, etc. . . .

5 www.e-travel.com Dienstleistungen und Lösungen.

6 www.checkmytrip.com.

7 http://www.amadeus.com/kundenprofile/x33913.html#.

8 http://www.amadeus.com/kundenprofile/x33911.html#StoryTen.

weg. Ich buche entsprechend seinen Wünschen und er holt die Unterlagen ab, sobald sie fertig sind. Kreditkartennummer, Adresse, Geburtsdatum, Reisepassnummer habe ich im Computer. Letztes Mal wäre das beinahe schief gegangen. Er hatte nach Verlust einen neuen Reisepass und wurde am Gate gründlicher als gewöhnlich kontrolliert. Dem Sicherheitspersonal fiel die abweichende Reisepassnummer auf. Schwierigkeiten waren die Folge. Nach einigem hin und her durfte er dann doch noch den Flieger nehmen. Jedoch hatte ihm diese Angelegenheit einige Schweißperlen auf die Stirn getrieben. Es lohnt sich, die Kunden regelmäßig nach solchen »Kleinigkeiten« wie z. B. Personalausweis oder Reisepass zu fragen.«

Sicher sind Erfahrungsberichte für Reisebüromitarbeiter notwendig, aber bitte schön nicht für jedermann. Derartige »Pannen« dienen jedoch als Anlass, das System immer detaillierter zu gestalten und alle Eventualitäten zu berücksichtigen. Dabei drängt der Wunsch nach Bequemlichkeit bei der Buchung den Schutz der Daten allzu schnell in den Hintergrund.

Die Systembetreiber werben mit folgenden Worten für Ihre Kundendatenbank, die demnächst eingeführt werden soll: »Willkommen bei Amadeus Customer Leisure Profiles. Amadeus Customer Leisure Profiles ist die ideale Lösung, wenn Sie Informationen über Ihre Leisure Kunden verwalten möchten. Mit dieser Kundendatenbank haben Sie alle relevanten Informationen im Beratungsgespräch direkt zur Hand. Mit einem Klick den Kunden im Blick: Sie können die Buchungshistorie und persönliche Daten Ihrer Kunden ganz bequem aufrufen und die Adressdaten direkt in Amadeus Tour Market (TOMA®) übernehmen. Das ist schneller, vermeidet fehlerhafte Eingaben und unterstützt Sie dabei, sich voll und ganz auf eine umfassende Beratung zu konzentrieren.« [9]

Der Schutz der Privatsphäre des Kunden wird überhaupt nicht in Erwägung gezogen; dass er eventuell Einwände bei der Datenübernahme haben könnte, wird völlig vernachlässigt. Daten, die bei früheren Buchungen oder in anderem Zusammenhang bereits erhoben wurden, werden ohne Kenntnis, geschweige denn Einverständnis des Kunden einfach in das neue System übernommen. Hier werden die Grenzen des Erlaubten ohne mit der Wimper zu zucken überschritten. Der Datenschutz wird förmlich mit Füßen getreten.

Schier skandalös mutet die Aussage an: »Alle relevanten Kundeninformationen auf einen Blick! Im Kundenprofil sehen Sie die Buchungshistorie, Kundendetails und Hobbys. Mit einem Klick können Sie dann die kundenbezogenen Felder in Amadeus Tour Market übernehmen.«

Kundendetails und Hobbys in einem weltweit eingesetzten Buchungssystem? Wie geraten solche Informationen in das System und was haben sie dort verloren?

Und es geht weiter mit fragwürdigen »aktiven Kundendaten«: »Bereits existierende Kundeninformationen aus Amadeus Customer Profiles (Air/Car/Hotel) stehen jederzeit aktuell zur Verfügung. Die Kundendaten aus der Auftragsverwaltung im Mid Office können automatisiert übernommen werden. Außerdem sind die Kundendaten für lange Zeit aktiv – egal wie alt die letzte Buchung ist. Von einer aktiven Kundenpflege bis zum nachhaltigen Erfolg: die Kundendaten inklusive Buchungshistorie bieten Ihnen die ideale Basis für eine effiziente Beratung!«

Wo bleibt das Recht auf informationelle Selbstbestimmung? Wie sieht es mit der Datensparsamkeit, wie sie vom Bundesdatenschutzgesetz gefordert wird, aus? Stellt man diese Fragen jedoch in einem Reisebüro, schaut man in erschrockene Gesichter. Auf die Frage, wo genau sich die Kundendaten befinden, erhält man die Antwort: »auf einem Server, dieser kann sich auch in Spanien in der Zentrale befinden, aber so genau wissen wir das nicht«. Es werden ja schließlich Reisen verkauft und mit EDV beschäftigt man sich nicht so intensiv, es reicht, wenn sie problemlos funktioniert.

Einen weiteren wichtigen Aspekt sollte ein Reisender berücksichtigen: der Kampf gegen den Terror geht wei-

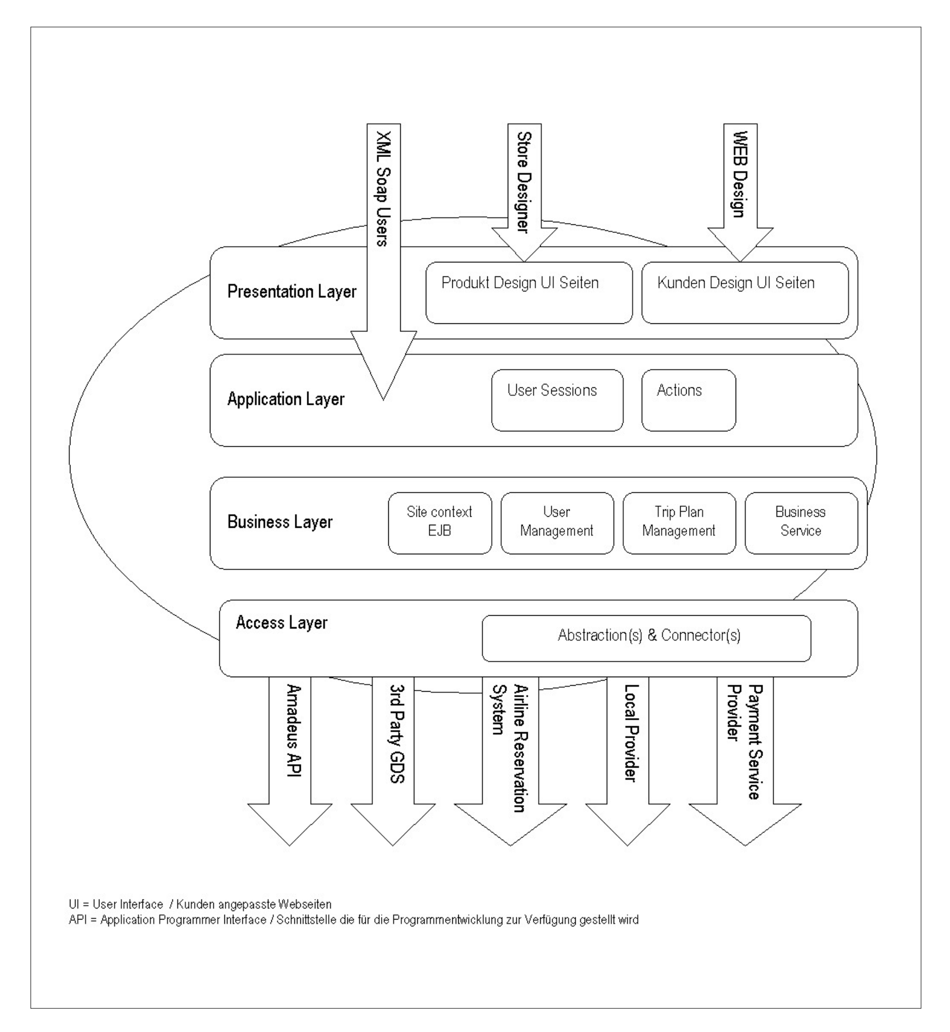


Abb. 1: Der **Amadeus »Global Connector«** dient als Schnittstelle zur direkten Anbindung in Flugbuchungssysteme sowie zur Anbindung an 3-Anbietersystem.

[9] Diese Informationen liegen dem Autor in Schriftform vor.

Amadeus

Amadeus, weltweit führender Anbieter im Electronic-Ticketing-Vertrieb, hat bisher die Ausstellung elektronischer Flugscheine (E-Tickets) für 153 Airlines und 138 Märkte ermöglicht – weit mehr als der Wettbewerb (Galileo, SABRE und Worldspan). Die Amadeus Germany GmbH, 1971 gegründet, hat ein umfassendes Angebot für den Vertrieb touristischer Leistungen aller Art über verschiedene Absatzkanäle wie Reisebüros, Call Center, Kartenvorverkaufsstellen oder Internet. Mit dem Bereich Corporate Solutions bietet das Unternehmen leistungsstarke Geschäftsreise-Lösungen für Travel Management in Unternehmen. Umfangreiche Trainingsmöglichkeiten runden das Portfolio ab. In Deutschland arbeiten 85 Prozent der Reisebüros an rund 40.000 PCs mit dem modernen, hoch entwickelten Amadeus-System. Alleiniger Gesellschafter von Amadeus Germany ist die Amadeus IT Group SA, ein weltweit führender Anbieter von Technologie- und Vertriebs-Lösungen für die Reise- und Tourismusbranche. Rund 78.300 Reisebüros sowie mehr als 11.500 Airline-Verkaufsbüros – und damit rund 400.000 PCs – in über 215 Märkten weltweit nutzen Netz und Datenzentrum von Amadeus.

Eine Spezialform der Reservierungssysteme stellt der Hotel Reservation Service (HRS) dar, der aus einer Datenbank mit 120.000 Hotels besteht, wovon in der Zwischenzeit 55.000 Hotels online zu buchen sind. HRS nutzt Amadeus ebenfalls als Reservierungssystem.

Seit 2002 existiert die Handelsplattform »Start Amadeus« (www.start.de), die mit Start PartnerNet auch einen Online-Dienst für die Touristikbranche anbietet. Reisebüros und Touristikanbieter, aber auch Verlage und Touristikzentralen, können darüber kommunizieren und gezielt Informationen austauschen.

ter, weshalb zu jeder abgegebenen Buchung eine eindeutige PNR Nummer (Passenger Name Record) vergeben wird. Diese Nummer und die dazugehörigen Informationen können von den in den USA für die Terrorabwehr zuständigen Behörden[10] (Department of Homeland Security) bei Flügen in die USA erfragt und dem Reisenden zugeordnet werden. Dies geschieht zwangsläufig beim Buchungssystem der gewählten Fluglinie. Aber auch die Behörden innerhalb der EU – Mitgliedsstaaten sind an diesen Informationen interessiert. Nach einer Klage des EU-Parlaments hat der EU-Gerichtshof[11] dem allerdings einen Riegel vor geschoben. Die Frage ist allerdings, wie lange dieser Riegel angesichts zunehmender Terrorismusgefahr hält.

Schnittstellen

Betrachtet man die einfache Darstellung der Datenflüss einnerhalb von Amadeus (vgl. Abb. 1), lässt sich erahnen wie komplex die Vorgänge bei einer Reservierung sind. Von der Reservierung über die Kontrolle der Kreditkartenabrechnung bis hin zur Einbindung der Daten in Fremdsysteme werden alle Informationen personenbezogen verknüpft.

Bei dieser Vielzahl an inneren und äußeren Schnittstellen stellt sich zwangsläufig die Frage: Wie wird die Vertraulichkeit der Kundendaten garantiert und wer darf eigentlich darauf zugreifen?

Geht man dieser Frage nach, gelangt man erschreckend schnell zu der Erkenntnis, dass noch nicht einmal das Intranet des Unternehmens[12] angemessen geschützt ist: Ohne große fachliche Kenntnisse gelangt man dort an Informationen, die nicht für jedermann bestimmt sind. Ein Zugang über eine gesicherte https-Verbindung wird scheinbar nicht für nötig gehalten. Ist das symptomatisch für den Umgang des Unternehmens mit Sicherheitsbelangen?

Im Geschäftsberichts der Amadeus Deutschland GmbH für das Jahr 2005 wird unter anderem darauf hingewiesen, dass bereits 99% der Reisebüros über das Internet Buchungen vornehmen.

»Im Bereich Airline-IT hat die Star Alliance einen Vertrag für eine gemeinsame IT-Plattform unterschrieben, der einen Meilenstein in der Geschichte von Amadeus darstellt. Zudem haben wir ein Portfolio an IT-Lösungen für Low-Cost-Carrier auf den Markt gebracht. Im Hotelbereich nutzen nun 6.500 Häuser unsere Technologie-Lösungen. Wir haben über 200.000 PCs in Reisebüros auf die browserbasierte Amadeus Selling Platform (Vista) migriert. Das heißt, über 99 Prozent der Reisebüros, die an das Amadeus System angeschlossen sind, arbeitet über Internet.«

Das bedeutet, dass in jedem dieser Reisebüros Mitarbeiter sitzen, die an alle bereits in einem Buchungssystem eingegeben Daten und Informationen über eine Person gelangen können. Diese Daten sind nur über die Reisebüronummer, den Benutzernamen und das Passwort über eine Internetverbindung abgesichert. Was das bedeutet, kann man aus der aktuellen Debatte um den »Bundestrojaner« ableiten. Mit Datensicherheit und Netzwerkschutz hat dies nicht mehr viel zu tun. Auch und gerade hier muss die Frage lauten: »Warum gibt es keine Hardware-Token oder ähnlich sichere Verfahren zur Authentifizierung? Und warum gibt es kein Berechtigungskonzept, das die Zugriffsmöglichkeiten von Nutzern auf »ihre« Kunden einschränkt?

Es ist erschreckend, wie einfach man sich die notwendigen Informationen besorgen und selbst in das Buchungssystem gelangen könnte. Man sieht der netten Dame im Reisebüro einfach beim Anmelden auf die Finger, notfalls (wenn das einfache »über die Schulter schauen« nicht schon ausreicht) mittels einer versteckten Kamera, die Videoaufzeichnung beherrscht. Das kann heute ja schon jedes bessere Handy.

Bedenkt man die Ergebnisse einer aktuellen Umfrage der Düsseldorfer Agentur Mediaedgecia , wonach bereits »35 Prozent der Deutschen mit Internetzugang ihren Last-Minute-Trip via Internet buchen«, dann kann man davon ausgehen, dass in absehbarer Zeit die Reisebranche all ihre Prozesse über das Internet mit allen seinen Sicherheitsmängeln abwickeln wird.

Und die Sicherheitsmängel bei den Clients der professionellen Dienstanbieter stellen nicht das einzige Problem dar. Denn wenn der Kunde direkt bucht, ist ebenfalls das Internet die bevorzugte Datenübermittlungsplattform.

Meistens werden die Last-Minute-Trips mit der Kreditkarte über nicht

---

10 http://www.datenschutz.de/feature/detail/?featid=3.

11 http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/77103.

12 http://www.amadeus.com/Corpweb/NewsItem2.nsf/a41e02bca618bb1b41256752004d0a6e/.

oder nur spärlich geschützte Internetverbindungen bezahlt. Somit befindet sich schnell eine stattliche Anzahl an Informationen und Daten über Reisende in diesem System. Ob diese Daten ausreichend geschützt sind, darf, wie oben ausgeführt, bezweifelt werden. Dass dieser Pool an Informationen über Kreditkartendaten, Handynummern, E-Mailadressen und viele andere Angaben eine willkommene Einladung für Datensammler darstellt, ist leider anzunehmen. Inzwischen geht die Branche der so genannten Informationsbeschaffer mit sehr professionellen Methoden zu Werke, um an verwertbare Informationen von Internetnutzern zu gelangen.

Die Unsichtbarkeit der Buchungssysteme

Sehr geschickt tarnen sich die Online-Reservierungssysteme der verschieden Anbieter. So werden von vielen Web-Seiten von Reiseanbietern über einen Link direkte Verbindungen mit dem Online-Reservierungssystem geschaffen. Dem Benutzer erscheint der Gesamtauftritt jedoch wie eine Einheit. Das Buchungssystem wird dem Webauftritt des Reiseanbieters angepasst, so dass keine Logos oder sonstige Informationen auf das eigentliche System hindeuten und so zu Irritationen führen. Sie glauben, das an dieser Stelle abgefragte Infomaterial oder die Reservierung der Urlaubsreise wird auf den Seiten des vermeintlichen Webanbieters vorgenommen? Sie irren sich! In Wirklichkeit erfolgen die Anfragen direkt in einem Buchungssystem, das alle Ihre Daten abfängt.

Datenschutzrechtlich handelt es sich bei dieser Einbettung des Buchungssystems um eine Datenverarbeitung im Auftrag gemäß § 11 BDSG. Ob die zwischen Auftraggeber (Reisebüro) und Auftragnehmer (Betreiber Buchungssystem) erforderliche strenge Vertragsregelung besteht, ist zweifelhaft. Denn in der Regel findet man noch nicht einmal einen Hinweis darauf, was mit den Daten geschieht und welche Wege sie nehmen. Auch ihrer Unterrichtungspflicht nach § 4 TDDSG kommen die Reiseanbieter häufig nicht nach. Auf den meisten Web-Seiten sucht man Datenschutzerklärungen vergebens. Findet man dann doch in seltenen Fällen Datenschutzerklärungen in einem versteckten Winkel der Website, sind diese meist nicht aussagekräftig.

Das Thema Datenschutz und Datensicherheit wird in der Reisebranche offensichtlich noch immer sehr stiefmütterlich behandelt.[13] Gründe dafür lassen sich viele vermuten. Der Hauptgrund scheint jedoch schlicht eine mangelnde Kenntnis der Rechtslage zum Thema Datenschutz und IT-Sicherheit zu sein. Dies lässt sich oft auch daran erkennen, dass wesentliche Grundpflichten nicht erfüllt werden, so z. B. die Erstellung des Verfahrensverzeichnisses. Und genauso selten haben sich die meisten Reiseanbieter bei ihrem Auftragnehmer von der Angemessenheit der ergriffenen technischen und organisatorischen Maßnahmen gemäß § 9 BDSG vor Ort überzeugt.

Wenn man Datenschutz als Qualitätsmerkmal begreift, mit dem man die Kundenbindung befördern kann, ist es nur ein kleiner Schritt zu Maßnahmen, die gesetzliche Vorgaben umsetzen und für Transparenz beim Kunden sorgen. Datenschutzerklärungen wirken dabei als vertrauensbildende Maßnahme, was der Verband Internet Reisevertrieb (VIR), ein Zusammenschluss großer deutscher Online-Reisebüros, glücklicherweise erkannt hat. Der Verband arbeitet mit dem unabhängigen Gütesiegel Safer-Shopping, das vom TÜV Süd vergeben wird. Zur Begründung der Siegelförderung bei seinen Mitgliedern fasst der Saferpay-Experte vom VIR zusammen:

»Ob Last-Minute-Reisen oder langfristige Urlaubsplanung, wer im Internet bucht, sollte dies bei Reiseanbietern machen, die durch eines der bekannten Gütesiegel wie Trusted Shops, Euro-Label oder Safer-Shopping zertifiziert sind. Und: Versenden Sie ihre Kreditkartendaten niemals per E-Mail!«

Fazit

Wenn einer eine Reise tut, dann kann er was erzählen. Noch viel interessanter wäre es, wenn unsere Daten erzählen könnten, welche Reisewege sie genommen und was sie erlebt haben, von wem sie angesehen wurden, wohin sie kopiert und verschoben wurden, wo, wie und wann Abgleiche stattgefunden haben und wozu sie sonst noch gebraucht und abgespeichert wurden.

Daten sollen laut Bundesdatenschutzgesetz zweckgebunden verarbeitet werden, kurz gesagt ist die Privatsphäre zu achten. Daten jeglicher Art sind insbesondere vor Ausforschung, Veröffentlichung und Nutzung durch Unberechtigte zu schützen. Hier hat die gesamte Reisebranche noch einen weiten Weg vor sich. Denn transparent und nachvollziehbar sind die Buchungsvorgänge keinesfalls, genauso wenig wie die Aussage in einem Reisebüro: »Ein Löschen Ihrer Informationen ist leider nicht möglich«.

In welchem Gesetz steht geschrieben, dass nach erfolgreichem Abschluss der Reise die meisten personenbezogenen Daten nicht gelöscht werden dürfen? Wo steht, dass Daten mit (z. B. steuerlichen) Aufbewahrungspflichten im produktiven System verbleiben und nicht archiviert werden dürfen? Ganz im Gegenteil: Dies ist gesetzlich sogar vorgeschrieben und sollte selbstverständlich sein. Darüber und über alle Fragen zum Datenschutz müssen sich die Reiseveranstalter in Zukunft Gedanken machen.

Bis dahin bleibt dem Reisenden nur die Möglichkeit, die Augen offen zu halten und trotz Urlaubsvorfreude nicht das eigene Persönlichkeitsrecht mit der Buchung abzugeben. Dass es auch anders geht, zeigt ein hoffnungsvoller Blick in die Schweiz: www.fairunterwegs.org.

---

[13] Vgl. hierzu auch den Erfahrungsbericht von »Oskar« in diesem Heft.

Oskar

Kreuzfahrten: Nichts für Datenschutzbewusste!

Ein Erfahrungsbericht

Das Angebot des Anbieters klang verlockend: Eine 12tägige Kreuzfahrt auf der Ostsee, attraktive Ziele und ein attraktiver Preis für eine Außenkabine.

Ein erstes Telefonat verlief zunächst erfreulich: »Die Kabine 612 ist verfügbar, soll ich für Sie buchen?« Meine Antwort »Ja, bitte für uns reservieren! Senden Sie mir die Unterlagen!« kam daher recht schnell.

Nach einigen Tagen erhielt ich dann bereits die Buchungsunterlagen, die auch einen Erfassungsbogen für das so genannte »Schiffsmanifest« enthielten. Hierbei handelt es sich um eine Sammlung von Passagierdaten für die Zoll- und Einreisebehörden, damit die Kontrolle vor Ort einfacher und schneller vor sich geht.

So gab ich also u.a. Name, Vorname, Geburtsdatum und -ort, Beruf, Reisepassnummer, Adresse und weitere geforderte Daten an.

Und wie das so ist, wenn man sich auf eine lang geplante Reise freut: die Vorbereitungen will man möglichst komplikationslos hinter sich bringen.

Während jedoch meine Unterlagen auf dem Weg zum zuständigen Regionalbüro des Reiseveranstalters waren, überkam mich doch die Neugier.

Wer speichert meine Daten und wer erhält sie wann und zu welchen Zwecken? Wo verbleiben meine Daten nach der Reise? Wer garantiert mir die datenschutzgerechte Verarbeitung und Nutzung? Kann ich bei allen besuchten Anrainerstaaten der Ostsee (darunter Russland) sicher sein, dass die Daten entsprechend den Vorgaben der EU-Datenschutzrichtlinie verarbeitet, geschützt und gelöscht werden?

Die Unterlagen meines Reiseveranstalters gaben keine Antwort auf meine Fragen. Weder hier noch auf der Homepage des Veranstalters finden sich diesbezügliche Hinweise oder eine Datenschutzerklärung.

Mein erneuter Griff zum Telefonhörer führte dann zu einem weniger erfreulichen Ergebnis. Da meine Fragen an der Buchungshotline offensichtlich nicht verstanden wurden, wünschte ich den Datenschutzbeauftragten des Veranstalters zu sprechen. Zu meiner Verblüffung wurde mir mitgeteilt, dass ein Datenschutzbeauftragter für das Unternehmen vollkommen »überflüssig« und »zu teuer« sei. Das folgende Streitgespräch, zunächst mit dem Vorzimmer, dann mit dem Geschäftsführer verlief nur teilweise sachlich und in der Form unbefriedigend.

Zusätzlich ärgerlich, dass eine telefonische Anfrage bei der zuständigen Aufsichtsbehörde mehr oder weniger mit dem Hinweis auf Zeit- und Personalmangel abgewürgt wurde: Für derartige »Kleinigkeiten« habe man keine Ressourcen.

Ein zweiter Gesprächsversuch mit der Geschäftsführung des Reiseveranstalters hatte dann schließlich ein Ergebnis – wenn auch ein anderes, als ich mir vorgestellt hatte: Fünfzehn Minuten nach Beendigung des Gesprächs klingelte das Telefon und das Regionalbüro teilte mir mit, dass auf Anweisung des Veranstalters unsere Teilnahme an der Kreuzfahrt abgelehnt worden sei.

Auf die Bestätigung der Löschung meiner personenbezogen Daten, die ich sofort anschließend schriftlich verlangt habe, warte ich noch immer ...

Nun hatte ich zwar etwas für meinen Datenschutz getan, jedoch plötzlich keine Aussicht mehr auf eine schöne Urlaubsreise. Ein glücklicher Zufall minderte meinen Schock, denn wir fanden eine ähnliche Reise bei einem anderen Reiseveranstalter.

Auch hier das gleiche Spiel: wiederum keinerlei Hinweise zum Datenschutz und keine Angaben, wie die erhobenen Daten verwendet würden. Doch diesmal wollte ich nicht erneut den Urlaub gefährden, sondern vorsorglich bis zum Ende der Reise stillhalten. Im Juli ging es schließlich los.

Und es kam, wie es kommen musste: Am Abend vor einem Landgang in St. Petersburg fand jeder Passagier neben der Aufforderung, die Reisepässe am Desk abzuholen, auch ein Formular des portugiesischen Reeders. Dieses fragte umfangreich personenbezogene Daten ab, die weit über das bei Buchung und für das Schiffsmanifest bekannte Maß hinausgingen. So wurde u.a. nach »Verheiratet mit ... seit« oder »Anreise mit ...« gefragt. Die Kombination dieser Abfrage mit der Passabholung habe ich als Ankündigung »Pässe gegen Daten« verstanden. Und so haben es viele Passagier wohl auch aufgefasst.

Das war mir jedoch zu viel der Neugier. Da mir niemand den Zweck dieser Datenerhebung und den Verbleib der Daten erklären konnte, weigerte ich mich laut und deutlich an der Passausgabe, das Formular abzugeben – und erhielt trotzdem meinen Pass. In der Folge taten es mir tatsächlich einige andere Passagiere in der Schlange nach, die die Diskussion mitbekommen hatten. Beim abendlichen Briefing wurde Datenschutz sogar ein Thema; doch da hatten die meisten anderen ihren Fragebogen treuherzig, besser treudoof, schon abgegeben. Pässe gegen Daten eben.

Nach der Heimkehr von einer ansonsten herrlichen und perfekt organisierten Reise auf einem exzellenten Schiff teilte ich dem Veranstalter mein Lob mit und nutzte die Gelegenheit, nun auch die Fragen nach dem Datenschutzbeauftragten und dem Datenhandling zu stellen. Die Sachlage war ähnlich unbefriedigend wie bei der Konkurrenz, aber immerhin konnte ich eine gewisse Aufgeschlossenheit gegenüber den grundsätzlichen Belangen und Erfordernissen des Datenschutzes heraushören. Dass dies nicht ausreichend ist, um die gesetzlichen Vorgaben zum Schutz Betroffener zu erfüllen, muss man nicht betonen.

Dennoch verkniff ich mir ein Nachkarten bei der Aufsichtsbehörde und dem ersten Reiseveranstalter – es hätte zwar meinem Ego gedient – doch auch dem Datenschutz? Da bin ich mir bei soviel erlebter Ignoranz, Unwissen und Desinteresse nicht sicher ...

Dr. Thilo Weichert, Leiter des ULD

ULD-Datenschutz-Tipps für Urlaubsreisende

Immer wieder wird bekannt, dass Daten etwa von Gästen in Hotels und Restaurants oder Kunden von Flug- und Reiseunternehmen in falsche Hände geraten, z.B. Daten zu Kreditkarten, mit denen im Urlaub bezahlt wird. Oft versuchen international agierende organisierte Kriminelle aber auch, Angaben aus Reisepässen, Personalausweisen, Führerscheinen sowie Reisedaten zu beschaffen, um sich unter Verwendung dieser Daten zu bereichern.
Die folgende Darstellung gibt – zum Beginn der Sommerurlaubszeit – Tipps, welche Sicherheitsmaßnahmen möglich und sinnvoll sind, um nicht das Opfer von Datenräubern zu werden.

Datenverarbeitung ist heute ein weltweites Geschäft, Computerkriminalität auch. Sog. Identitätsdiebstahl, d.h. die Beschaffung von Identitäts- und Kreditkartendaten und das Abheben von Geld oder das elektronische Bezahlen unter dem falschen Namen, ist z.B. in den USA zu einem riesigen gesellschaftlichen und wirtschaftlichen Problem geworden. Es besteht immer ein gewisses Risiko, dass die eigenen Daten, die man während des Urlaubs offenbart, missbraucht werden. Ob dies tatsächlich passiert, hängt von der Vertrauenswürdigkeit des Restaurants, Hotels, Veranstalters usw. ab, dem man seine Daten zur Verfügung stellt. In Deutschland gibt es strenge Datenschutzgesetze und eine funktionierende Datenschutzaufsicht. Daher ist hier das Risiko geringer als in anderen Ländern, und die Chance, dass ein Täter erwischt wird, ist höher.

In Hotels müssen in Deutschland – und ähnlich ist es in fast allen anderen Staaten – sog. Meldescheine ausgefüllt werden: Name und Vorname, Adresse, Geburtsangaben und Nationalität, Anreise- und Abreisetag – mehr nicht. Die Daten bleiben im Hotel, müssen aber auf Anfrage der Polizei zur Verfügung gestellt werden.

Autoverleihfirmen und sonstige Dienstleister erheben jeweils die Daten, die nötig sind zur Identitätsfeststellung und zur Abwicklung von Problemfällen, z.B. wenn ein Unfall passiert oder etwas abhanden kommt. Unter Umständen versucht sich das Unternehmen Sicherheiten zu beschaffen. Erhoben werden dürfen immer nur die Daten, die zur Identifizierung oder zur Risikoabsicherung erforderlich sind.

Beispiel: Die Vorlage des Passes oder Personalausweises ist dann in Ordnung, wenn die Identität zur Sicherheit eindeutig festgestellt werden muss; eine Kopie ist dagegen nicht nötig; auf der Kopie des Dokumentes sind nämlich mehr Infos enthalten, z.B. über frühere Reisen, die Ordnungsnummer oder biometrische Daten. Das Erstellen von Ausweiskopien bedarf also der ausdrücklichen und freiwilligen Zustimmung des Gastes. Die erhobenen Daten müssen in jedem Fall vertraulich behandelt werden, d.h. sie dürfen nicht einfach an Dritte weitergegeben werden. Zulässig ist aber, die Daten für eigene Werbezwecke zu nutzen.

Mit der Angabe von Kreditkartendaten sollte man sehr vorsichtig sein. Unter keinen Umständen darf die persönliche Identifizierungsnnummer, die PIN, bekannt werden, weder über Internet noch am Telefon, weder durch Beobachten beim Eintippen am Automaten noch durch einen Merkzettel im Geldbeutel. Wird eine EC-, Kredit- oder sonstige Berechtigungskarte gestohlen oder kommt diese abhanden, so sollte sie umgehend gesperrt werden. Nach Rückkehr aus dem Urlaub sollte in jedem Fall das Konto daraufhin überprüft werden, ob es nicht zu unberechtigten Abbuchungen gekommen ist. Wenn ja, sollten diese sofort rückgängig gemacht werden.

Generell sollte folgender Tipp beachtet werden: Menschen und Stellen, die man nicht kennt und denen man nicht vertraut, nur das Allernötigste offenbaren. Erscheinen bestimmte Fragen dubios, unbedingt nachfragen, was das soll. Es macht Sinn, eher auf ein Angebot zu verzichten als persönliche Angaben zu machen, die den Gegenüber nichts angehen und die möglicherweise missbraucht werden können. Besteht der Gegenüber auf bestimmten Angaben und will man auf ein Angebot nicht verzichten, ist es auch möglich, Phantasieangaben zu machen. Dies ist zulässig, es gibt also ein »Recht auf Lüge«, wenn die Angaben für den Vertragsabschluss nicht benötigt werden.

Der wichtigste Tipp ist: Datenspuren vermeiden: Bargeld ist anonym, Kartenzahlungen sind es nicht. Oft akzeptieren aber Hotels oder Veranstalter nur noch Kartenzahlungen. Dann muss man entscheiden, ob man das nötige Vertrauen hat. In jedem Fall sollte man die Karte nicht völlig aus der Hand geben, so dass sie z.B. auch nicht in einem Hinterzimmer kopiert werden kann.

Kaum eine Möglichkeit der Datenvermeidung besteht bei Flugreisen. Tickets werden in der Regel nur personifiziert ausgestellt. Beim Check-In erfolgt eine eindeutige Identifikation anhand von Pass oder Personalausweis. Doch sind seriöse Fluggesellschaften – nach einigen bekannt gewordenen Skandalen – bestrebt, die Fluggastdaten vertraulich zu behandeln. Faktisch ist dies bei Flügen, die einen Bezug zu den USA haben, nicht gegenüber den US-Behörden möglich. Diese zwingen unter dem Vorwand der Terrorismusbekämpfung die Fluggesellschaften dazu, einen sog. Passenger Name Record (PNR) mit 34 Einzelangaben herauszugeben: neben Name und Adresse z.B. Buchungs-, Zahlungs- und Kreditkartendaten, Angaben zur Flugroute und Begleitpersonen, E-Mail- und Telefonnummer. Es sind Fälle bekannt geworden, dass anhand dieser Daten die US-Behörden Reisende abgecheckt und dann an der Grenze abgewiesen haben.

Welche Formen des Datenmissbrauchs sind möglich?

Der klassische Schaden für den Normalbürger ist, dass mit den Kreditkartendaten das Konto geplündert wird. Auch durch zeitnahe Kontrolle der Kontobewegungen und der sofortigen Meldung des Verlustes einer EC- oder

Kreditkarte kann der Schaden nicht immer begrenzt werden. Abwesenheitsinformationen können dazu genutzt werden, zu Hause die Wohnung auszuräumen. Der Phantasie von Kriminellen sind leider keine Grenzen gesetzt: Kompromittierende Urlaubsdaten können zur Erpressung genutzt werden. Bei Prominenten können Urlaubsindiskretionen bis hin zu üblen Artikeln z.B. in einem Boulevardblatt führen.

Welche Hilfemöglichkeiten gibt es, wenn mit den eigenen Daten etwas falsch gelaufen ist?

Inzwischen gibt es in allen europäischen und vielen anderen Ländern Datenschutzkontrollinstanzen, bei denen man sich bei Datenmissbrauch beschweren kann und die Verstöße aufklären und ahnden können. Die Adressen der zuständigen Instanzen sind im Internet im Virtuellen Datenschutzbüro zu finden unter www.datenschutz.de/institutionen.

Bei kriminellen Machenschaften ist der Gang zur örtlichen Polizei zu empfehlen, die aber in Sachen Datenschutz oft nicht die nötige Erfahrung hat. In jedem Fall sollte man vor Ort bei dem Unternehmen, also z.B. beim Verantwortlichen im Hotel, Aufklärung einfordern. Soweit es in den Ländern Datenschutzgesetze gibt, enthalten diese durchgängig einen Auskunftsanspruch der Betroffenen gegenüber dem Unternehmen. In jedem Fall sollte auch der Reiseveranstalter bei Unregelmäßigkeiten eingeschaltet werden.

Wenn das oben Gesagte beachtet wird, ist das Risiko eines Datenmissbrauchs gering. Aber: eine hundertprozentige Sicherheit gibt es nicht. Dies sollte aber Niemanden daran hindern, in den Urlaub zu fahren. Das ULD wünscht allen keine bösen Überraschungen, viel Spass und gute Erholung.

Dieser Text findet sich im Internet unter www.datenschutzzentrum.de/allgemein/urlaubsreisende.htm.

This is an ePassport

This passport contains a microchip which stores the same information as appears on the data page. The chip can be read electronically to confirm the identity of the bearer. This document complies with International Civil Aviation Organisation standards and incorporates security features to prevent illegal access to the information stored on the chip. See the centre page of the passport for further information.

Protect your identity

Lost or stolen passports provide criminals and terrorists with the opportunity to assume another identity, travel illegally and commit crimes. You must report the loss or theft of your passport without delay. *A lost or stolen passport will be immediately and permanently cancelled. It must not be used again under any circumstances.*
Lost or stolen passport information is shared with other countries and use of a cancelled passport may result in denial of entry to overseas countries and disruption of travel plans.
To replace a lost or stolen passport, you will need to pay an additional fee on top of the normal application fee. In cases of multiple losses the replacement passport may be restricted in validity.

The Australian Passports Act 2005 imposes tough penalties on anyone using a cancelled passport.

Your passport identifies you – protect it at all times.

CHIP CENTRE PAGE

This passport contains sensitive electronics. For best performance, please do not bend, perforate or expose to extreme temperatures or excess moisture.

This passport contains a contactless integrated circuit chip which is an electronic device. In addition to the normal care and respect afforded a passport, please regard this document as you would any other portable electronic device, by ensuring that it does not become wet, folded or mutilated. Abuse may adversely affect the operation of the chip and reduce its utility to the bearer and to border inspection personnel.

DO NOT STAMP THIS PAGE

17

Sicherheitswarnungen im australischen RFID-Reisepass

Leon Hempel

Die Neue Überwachung – internationale Experten diskutierten eine adäquate Bewertung

Die Tagung »The New Surveillance« in Berlin, 30.11. – 1.12.2006

Bereits 1989 hatte der amerikanische Kommunikationswissenschaftler Oscar Gandy festgestellt, dass der Begriff der Informationsgesellschaft übersehe, dass es sich dabei im Kern um eine Überwachungsgesellschaft handle. Ein gutes Jahrfünft später konstatierte der britische Stadtsoziologe Stephen Graham, dass sich Videoüberwachung zur fünften Säule städtischer Infrastruktur entwickele. Inzwischen lässt sich feststellen, dass Überwachungsinfrastrukturen einen Grad an Normalität erreicht haben wie eben Wasser, Gas, Kommunikation und Entsorgung. So heißt es in dem vom Britischen Datenschutzbeauftragten in Auftrag gegebenen, kürzlich in London präsentierten »Report on the Surveillance Society«[1], dass das Szenario der Überwachungsgesellschaft nicht mehr Zukunftsmusik sei, sondern bereits Realität. In sämtlichen Industrienationen hätten sich Praktiken der Überwachung auf der Grundlage von Informations- und Telekommunikationstechnologien etabliert, die sich durch eine dauerhafte Erhebung und Nutzung von persönlichen Daten auszeichne, 24 Stunden am Tag und 7 Tage in der Woche. Unter dem neuen Paradigma eines »living with risk« verhallt dabei der Appell von kritischen Beobachtern an Politik und Wirtschaft, die Freiheitsrechte der Bürger zu achten. Stattdessen breitet sich »ein Klima der Alltäglichkeit der Beobachtung und der Gewöhnung an Überwachung« aus, wie jüngst Hamburgs Datenschutzbeauftragter Hartmut Lubomierski treffend befand.[2]

Am Zentrum Technik und Gesellschaft der Technischen Universität Berlin fand Anfang Dezember 2006 die Tagung »The New Surveillance« mit rund 100 Teilnehmern aus Wissenschaft, Kunst und interessierter Öffentlichkeit aus 15 Nationen statt.[3]

Gegenstand der zweitägigen Tagung war die Frage nach der Agenda der Überwachungserforschung. Nicht das Ob der Überwachungsgesellschaft stand zur Debatte als vielmehr, wie dem Thema methodisch zu begegnen ist: Nach Einschätzung der Initiatoren erschwert die rasante technologische Entwicklung eine adäquate Bewertung. Sei man einerseits mit einer Fülle von technologisch unspektakulären Einzelanwendungen im privaten und öffentlichen Bereich konfrontiert, stelle die Einbettung von Verfahren wie Biometrie oder RFID in visuelle Überwachungstechnologien bereits die Überwachungstechnologie der nächsten Generation dar, wenn ein Generationenschema angesichts des technologischen Entwicklungstempos überhaupt noch Sinn machte. Interaktive Systeme ließen nicht nur die Menge an erfassten Daten exponentiell ansteigen, sondern entzögen zugleich die Datenströme der Nachvollziehbarkeit. Das Problem methodischer Bewältigung bestünde hier schon darin, die einzelnen Systemkomponenten so zu identifizieren, dass festgestellt werden kann, wie sie zum Gesamteffekt beitragen.

Dass wir uns »schlafwandelnd« in der Überwachungsgesellschaft einfinden, meinte auch der Bundesdatenschutzbeauftragte Peter Schaar in seinem Einführungsvortrag. Unter unterschiedlichsten Zielvorgaben betreffe die neue Überwachung jeden einzelnen, sei es »as citizen, as banking client, as consumer, as internet user, as driver, as a potential criminal, or as a passenger«. Der stetig wachsende Umfang registrierter persönlicher Daten basiere auf einer Anhäufung teils neuer, teils erweiterter Technologien in einem Prozess, der sich durch die Integration von Technologien und Systemen ständig beschleunige. Machen die Technologien Überwachung zwar erst möglich, liege andererseits aber ein politikökonomischer Wandel der Entwicklung selbst zugrunde. Schaar wies darauf hin, dass nicht zuletzt die Globalisierung und die innere Grenzenlosigkeit Europas auch bei der noch unzureichend beantworteten Frage der Kontrolle der neuen Überwachung einen entscheidenden Horizont bilden.

Definitionen und Theoriebildung

Mit dem Ziel, den Überwachungsstudien begriffliche Schärfe zu verleihen, standen theoretische (Vor)-Überlegungen im Zentrum mehrerer Vorträge. Didier Bigo, Professor für Internationale Beziehungen an der Pariser Universität Sciences-Po, setzte bei dem technologischen Versprechen an, auf Grundlage einer technologie-basierten Grammatik des »future antérieur« Gefahren im Vorfeld abwehren zu können. Laut Bigo setzten sich darin administrative Ausnahmeregelungen und proaktive Polizeistrategien durch. Ziel von Überwachung sei es, die des antizipierten Verhaltens Verdächtigten vorzeitig von kritischen Orten und Infrastrukturen auszuschließen. Identitäten und Verhaltensweisen, die nicht oder noch nicht realisiert seien, erhielten durch die in die Kontrollapparaturen eingeschriebenen Algorithmen der vorweggenommenen Bedrohungserkennung einen paradoxen Status von Gegenwart. Getrieben von dem Glauben an eine omnipräsente Gefahr terroristischer Anschläge würden diese Strategien gesellschaftsfähig. Mit der Routinisierung der proaktiven Maßnahmen werde die neue Überwachung unter den Blicken einer paralysierten Öffentlichkeit zur Normalität. Unter dem Zeichen der Präven-

[1] online unter: http://ico.crl.uk.com/files/Surveillance%20society%20full%20report%20final.pdf.

[2] Die Tageszeitung (26.1.2007).

[3] Abstracts der Beiträge finden sich auf der website der Konferenz: http://www.ztg.tu-berlin.de/surveillance/abstracts.html.

tion werde die »Ausnahme zur Regel«, zu einer Technik des Regierens, bei der die politische Verantwortung letztlich an die automatisierten Verfahren der Kontrolle und Überwachung abgegeben ist.

Daran anschließend skizzierte Thomas Mathiesen, Rechtssoziologe von der Universität Oslo an Beispielen transnationaler Überwachungsnetzwerke wie dem Schengener Informationssystem, Europol und Echelon ein im Entstehen begriffenes »lex vigilatoria«[4]. Dieses setze sich einerseits von der sozialen und vor allem politischen Verfasstheit demokratisch regierter Staaten zunehmend ab, wirke zugleich aber norm- und regelsetzend auf die Gesellschaften zurück. Mathiesen zeigte auf, wie ein globales System polizeilicher Zusammenarbeit und Überwachung entstehe, das sich von nationalstaatlicher Verfassungsmäßigkeit entbindet und selbstreferentiell und selbst validierend konstituiert. Nicht mehr der Staat, nicht mehr demokratisch legitimierte Parlamente, sondern »quasi-legislative Institutionen« entschieden über die Überwachungsmechanismen.

Lucas Introna von der Manchester University Management School fokusierte in seinem Vortrag zu den ethischen und politischen Implikationen von Überwachungssystemen die Betrachtung und das Verstehen der Systeme und ihrer Wirkungen. Dabei wies er zunächst Ansätze zurück, die diese Fragestellungen entweder im Sozialen, beim Anwender oder in der Domäne der Technik selbst suchten. Es greife, gerade wenn es um algorithmische Überwachungssysteme wie Gesichtserkennung gehe, zu kurz, ethische Probleme entweder in einem normativ zweifelhaften Nutzen der Technik zu verorten oder in der Technik selbst, die zu einem fragwürdigen Nutzen zwänge. Vielmehr sei es notwendig, einen »co-constitutiven« Begriff von Technik zu entwickeln, einen Ansatz, der die Dimension des Sozialen mit der Domäne des Technologischen von vornherein verknüpfe. Solches Denken in soziotechnischen Konstellationen orientiere sich an der Simultaneität von Intentionen, Entscheidungen, Interpretationen und Nutzungen einerseits, die sozial wie kulturell determiniert sein könnten, und zugleich an den sozialen Einschreibungen in Codes und technologische Verfahren. Das Nebeneinander bestehender Ansätze müsse zu einem integrierten sozio-technischen Bewertungskonzept erweitert werden. Erst dann ließe sich nicht nur der Status quo der Überwachung bewerten, sondern auch proaktive Regulationstechniken erwägen, die angesichts der immer extensiveren und intensiveren Überwachung geboten seien.

Überwachung und Evaluation

Intronas Plädoyer spiegelte sich in den empirisch orientierten Beiträgen wider. So war man sich einig, dass bisherige Evaluationen zu kurz griffen, ja, dass unabhängig von ihren Ergebnissen Evaluationen häufig nur Teil der politischen Agenda der Durchsetzung von Überwachungstechnologien seien. Wie der kanadische Sozialwissenschaftler Kevin Haggerty in seinem Beitrag feststellte, könne bei den meisten Evaluationen von ergebnisoffener Bewertung nicht die Rede sein. Bemühungen, Effektivität von Überwachungsmaßnahmen zu evaluieren, liefen in erster Linie darauf hinaus, öffentlichkeitswirksame Statements wie »introducing CCTV cameras reduced car thefts by 8%« oder »Biometric Cards reduced vandalism by 12%« zu produzieren. Tatsächlich hätten die Ergebnisse von Evaluationen selbst nicht einmal eine Wirkung auf den tatsächlichen politischen Entscheidungsprozess. Nicht nur werde in der Regel ein fragwürdiges Design nach Maßgabe der amerikanischen Kriminalpräventionsforschung angewandt, das das komplexe Zusammenspiel von Technik, Anwendung und Kontexte auf Erfolg und Nicht-Erfolg in fragwürdigen Dimensionen reduziere. Vielmehr schreite die Einführung und Erweiterung von Überwachungsmaßnahmen unabhängig von Evaluation frei nach der Strategie »success by failure« voran.

Sander Flight vom Crime Prevention Council Amsterdam zeigte anhand von mehreren in den Niederlanden durchgeführten Evaluationen – für die Zuhörer Haggertys wenig überraschend – auf, dass ihre Ergebnisse keine zuverlässigen Rückschlüsse zuließen und Erfolg oder Nicht-Erfolg eines Systems nicht verallgemeinerungsfähig seien. Während in Amsterdam und Rotterdam zwar beispielsweise die Kriminalitätsrate nach Einführung von Videoüberwachung gefallen sei, sei sie in Utrecht und Arnheim stattdessen gestiegen. Und während in Arnheim und Rotterdam die Kriminalitätsfurcht an den überwachten Orte gefallen sei, habe man in Utrecht und Amsterdam diesbezüglich keine Veränderung feststellen können. Unter Rückgriff auf Konzepte der so genannten »realistic evalution« unterstrich Flight die Bedeutung der kontextgebundenen öffentlichen Wahrnehmung von Sicherheit und Überwachung. Die Mehrzahl der landläufig vermuteten Effekte wie etwa der Verbesserung des subjektiven Sicherheitsempfindens oder der Abschreckung durch Kameras beziehe sich unmittelbar auf diesen regelmäßig missachteten Aspekt. Gerade der Einfluss auf Kriminalitätsangst sei nachweislich davon beeinflusst, ob und wie die Öffentlichkeit Kameras im öffentlich zugänglichen Raum überhaupt wahrnehme.

Durch mehrere folgende Tagungsbeiträge wurde zunehmend deutlich, was auf Agenden von Evaluationen nicht zu finden ist. Wie soziale Ordnung garantiert werden solle, zeigte die Architektin von der Technischen Universität Berlin Anke Hagemann am Berliner Olympiastadion. Bereits in der Anordnung des Stadions manifestiere sich Kontrolle im Sinne panoptischer Überwachung. Anhand von Bildmaterial und Interviews konnte sie detailliert aufzeigen, dass unter dem Signum der Sicherheitsanforderungen bei der baulichen Planung, Umsetzung und Implementierung von Sicherheitstechnologie weit mehr Aspekte eine Rolle spielten als die Produktion von Sicherheit. Kontrolle auf Grundlage der Stadienarchitektur umfasse die Einteilung von Menschenmassen in ökonomische und soziale Gruppen mit der Folge von Individualisierung, Ausgrenzung und – nicht zuletzt durch das Anbieten spezieller Konsumangebote – Privilegierung. Hagemann unterstrich damit, dass Kontrolle, vergleichbar der Privatisierung von Innenstadträumen, vor allem auch sozio-ökonomisch zu denken ist.

Gestützt auf britische Studien sowie eigenen Untersuchungen zur Videoüberwachung in Oslo und Kopenhagen verglich Heidi Mork Lomell von der Universität Oslo die Praxis von Überwachung im privaten und öffentlichen Bereich. Dabei offenbare der Vergleich, dass der Einsatz von Videoüberwachung von organisatorischen und kulturellen Aspekten geformt wird. Gerade hinsichtlich der Generierung von Verdacht konnten in allen Untersu-

[4] Vgl. zu Mathiesen auch online: http://www.heise.de/tp/r4/artikel/6/6861/1.html.

chungsfällen bei nicht-teilnehmender Beobachtung in Kontrollräumen Elemente von Diskriminierung nachgewiesen werden. Gerieten die ›üblichen Verdächtigen‹ ins Visier der Überwachung, erfolge durch die Überwachung eine Form von sozialer Sortierung. Je nach kulturellem Kontext und Zweck der Überwachung ließen sich aber auch unterschiedliche Verdachtsmuster bei der Beobachtung aufzeigen, die zum Teil auch unterschiedliche Strategien etwa beim Zugriff auf die Verdächtigen nach sich zögen.

Überwachung und Verhalten

Clive Norris, Kriminologe an der Universität Sheffield, unterstrich, dass sich durch die Technisierung sozialer Kontrolle die Polizeiarbeit ebenso wie das Verhalten der Bürger verändere, weil in das Interaktionsgefüge zwischen Kontrollinstanzen und den Kontrollierten eingegriffen werde. Soziale Interaktion werde abstrakter, wobei die Automatisierung der Überwachung eine maximale Distanz zwischen den Organen und den Bürgern schaffe, die das Risiko berge, der Garantie oder der Wiederherstellung der sozialen Ordnung gerade zuwiderzulaufen.

Martin Gill, der den Einsatz öffentlicher und halböffentlicher Videoüberwachungssysteme unter anderem im Auftrag des Britischen Home Office in einer Metaevaluation untersuchte, fragte danach, wie es sein kann, dass sich die Überwachung einerseits immer weiter ausbreitet, wenn ihr Erfolg auf der anderen Seite zweifelhaft ist. Für den Britischen Kriminologen liegt der Grund hierfür weniger in den technischen Anwendungen als vielmehr im mangelhaften Management der Systeme. »CCTV doesn't work, if it's not managed properly.« Gill fokussierte zur Stützung seiner These insbesondere das Verhalten der Täter, das – merkwürdig genug, bedenkt man die Zielvorgaben der Überwachung – in Untersuchungen regelmäßig nicht untersucht werde. Was Gill anhand von Täterbefragungen nachweisen konnte und am Beispiel von Überwachungssystemen von Kaufhäusern aufzeigte, ist, dass sich Überwachungssysteme mit Flucht-, Leugnungs-, Ablenkungs- und Streitstrategien spielend überlisten lassen. Anhand von Interviews konnte nachvollzogen werden, dass Täter Kameras entweder vollständig ignorierten oder, vorausgesetzt sie handelten nicht affektgesteuert, die Instrumente der Überwachung wie andere Tatgelegenheitsstrukturen bei der Planung mit einbezögen. Es bleibt allein die Frage offen, ob die von Gill angemahnte mangelnde Organisation nicht auch dahin gehend interpretiert werden müsste, dass Systeme – wie stets – Widerstand mit produzierten und sich nicht trotz, sondern gerade wegen ihres zweifelhaften Erfolgs immer weiter ausbreiteten.

Nils Zurawski legte schließlich den Fokus auf die Wahrnehmung von Sicherheit und Überwachung in der Bevölkerung. Es ist bekannt, dass Überwachungsmaßnahmen in der Bevölkerung in der Regel auf breite Akzeptanz stoßen. Zugleich wissen wir, dass das subjektive Sicherheitsempfinden durch die Präsenz von Kameras aber nicht erheblich beeinflusst wird, wie auch Sander Flight in seinem Beitrag am Beispiel Amsterdams nachwies. Zurawski wies mit der Methode des sog. mental mapping nach, dass die Wahrnehmung von Sicherheit grundsätzlich im Zusammenhang mit der konkreten Erfahrung von räumlichen Struktur steht. Unsicherheitsgefühle beruhen ebenso wie die Wahrnehmung von Überwachung in der Regel nicht auf objektivem Wissen, sondern vielmehr auf einer meist diffusen, subjektiven Wahrnehmung des Raums.

Überwachung und Regulation

Hatte Peter Schaar eingangs die Notwendigkeit der Kontrolle von Überwachung angemahnt, wurde die Frage, wie Überwachung zu regulieren ist, in den Beiträgen von Gerit Hornung von der Universität Kassel und Charles D. Raab von der Universität Edinburgh aufgegriffen. Beide unterstrichen, dass Regulierung zunächst einmal Aufmerksamkeit hinsichtlich der unterschiedlichen Effekte von Überwachung erforderlich macht. Regulierung sei im Ergebnis nicht nur von Gesetzgebung und Rechtsprechung zu leisten, sondern müsse, so Hornung heute bereits am technologischen Design selbst ansetzen, um bei der Genese der Überwachungssysteme regulative Standards in die Technologien mit einzuschreiben.

Charles Raab, Mitverfasser des »Report on the Surveillance Society«, ging von einem angelsächsischen Standpunkt aus darüber hinaus. Was bislang fehle sei eine präzisere Formulierung der Ziele von Regulierung und eine Analyse, wie diese Ziele mit den Techniken von Überwachung verbunden werden könnten. Es sei nach wie vor nicht klar, bis zu welchem Grad es individuell und gesellschaftlich tolerierbar sei, in die Privatsphäre einzugreifen und wie Regelungen, ›Codes of practice‹ und ähnliches zu einer Limitierung und Kontrolle von Überwachung tatsächlich beitragen. Es bedarf zudem eines Ansatzes, der über »privacy« hinausgehe, da neben indvidualrechtlichen auch gesellschaftspolitische Werte wie Gleichheit und Freiheit von Diskriminierung durch die neue Überwachung auf dem Spiel stünden. Dies würde bedeuten, dass man in die Problemstellung der Regulierung die Erforschung sozialer Prozesse und Auswirkungen neben der Befolgung und Kontrolle von Datenschutz-Standards mit einbeziehen müsse. Dabei sei es selbstverständlich ebenso notwendig, die unterschiedlichen Maßstabsebenen der Politik, von der lokalen über die nationale und europäische bis zur globalen Ebene, mit einzubeziehen. Raab plädierte in seinem Vortrag, das »Privacy Impact Assessment«, also inwiefern Privacy-Aspekte bei der neuen Überwachung berücksichtigt seien, zu einem »Surveillance Impact Assessment« zu erweitern. Nur so könne langfristig eine angemessenen Regulierung der aktuellen und künftigen Überwachungsformen erreicht werden, die auch die Balance zwischen Sicherheitsbedarf und Freiheitsrechten garantiere.

Thilo Weichert

Weshalb das Personenkennzeichen in der Sportsicherheit unerlässlich ist

Anmerkung zu dem Verfahren zwischen einem datenschutzbewussten Fußballfan und dem Deutschen Fußballbund e.V. wegen der Speicherung der Personalausweisnummer

1. Der DFB-Datenbankabgleich

Es ist schon verblüffend, wie viele Datenschutzverstöße möglich sind, ohne dass diese geahndet werden, wenn nur kein politischer Wille zur Ahndung besteht. So ließe sich das Verfahren zusammenfassen, das ein Fußballfan aus Dresden mit der Unterstützung des FoeBuD gegen den Deutschen Fußballbund e.V. (DFB) durchführte, um die Löschung seiner Personalausweisnummer in einer DFB-Datenbank zu erreichen.

Ihre Personalausweis- bzw. Passnummer mussten alle angeben, die ein Ticket für die Fußball-Weltmeisterschaft (WM) haben wollten. Ziel war die eindeutige Identifizierung der StadionbesucherInnen für Sicherheitszwecke. Die Eintrittskarte war mit einem RFID-Funk-Chip ausgestattet, über den beim Stadioneinlass eine Datenbank abgefragt werden konnte, in der die Personalien und eben die Ausweisnummern der TicketkäuferInnen gespeichert waren. Die StadionbesucherInnen sollten ihre Identität mit ihrem Personalausweis nachweisen. Der Abgleich von dessen Nummer mit der in der DFB-Datenbank gespeicherten Nummern sollte bestätigen, dass die das Ticket besitzende und sich ausweisende Person auch die zum Ticketbesitz und zum Spielbesuch berechtigte Person ist.

2. Die Argumente des Klägers und des Datenschutzes

Das Argument des Klägers war im Grunde einfach. Er berief sich auf § 4 Abs. 2 Personalausweisgesetz (PersAuswG), der es verbietet, die Seriennummer des Personalausweises so zu verwenden, »dass mit ihrer Hilfe ein Abruf personenbezogener Daten aus Dateien oder eine Verknüpfung von Dateien möglich ist«. Nach § 4 Abs. 3 PersAuswG darf der Ausweis generell durch private Stellen »weder zum automatischen Abruf personenbezogener Daten noch zur automatischen Speicherung personenbezogener Daten verwendet werden«. Was nicht nur für den Laien, sondern auch für einen Juristen eigentlich klar ist bzw. war, sollte offiziell nicht klar sein, nämlich, dass die DFB-Praxis gegen diese Regelung verstößt bzw. verstieß.

Nicht weniger klar sollte eigentlich auch die zweite Argumentationsschiene sein, die der Vertreter des Klägers vorbrachte, nämlich dass für den Zweck sicherer Spiele die Nummernspeicherung nicht erforderlich ist. Zwar ist das mit der Sicherheit immer so eine Sache – man weiß immer erst hinterher genau, dass die Sicherheit in Gefahr war – oder auch nicht. Doch war ExpertInnen offensichtlich, dass das Personalisierungskonzept des DFB nicht aufgehen konnte: Schwarzmarkttickets waren zu Hauf auf dem Markt. Offiziell wurde auf die Personalisierung von Tausenden von Eintrittskarten verzichtet. Eine Prüfung mit Ticket und Personalausweis unter Abfrage der DFB-Datenbank wäre schon aus praktischen Erwägungen nicht durchführbar gewesen – sie wurde auch nicht durchgeführt.

Dennoch hatte die zuständige Datenschutzaufsichtsbehörde in Hessen das Verfahren abgesegnet, unter der Auflage, dass bei der Programmgestaltung der DFB-Datei eine Ordnung nach oder eine Suche mit der Personalausweisnummer nicht möglich ist (vgl. Hornung DuD 2006, 434). Diese Auflage war das Ergebnis von Verhandlungen zwischen der Behörde und DFB bei dem Versuch, von vornherein Festgelegtes (Personalisierung mit Ausweisnummer) so zu drehen, dass der Gesetzesverstoß nicht ganz offensichtlich ist. Auch mit den anderen Anforderungen nahm man es nicht so ernst, wenn es darum gehen konnte, der großen Fußballweltmeisterschaft kleine Datenschutzsteinchen in den Weg zu werfen. Ein Schelm ist der, der diese eigenmächtige Position der besonderen Unabhängigkeit der unter Aufsicht des hessischen Innenministeriums stehenden Aufsichtsbehörde zuzuschreiben versucht.

3. Amtsgericht Frankfurt am Main

Das Amtsgericht wies die Klage des Fußballfans aus Dresden auf Löschung der Personalausweisnummer mit Urteil vom 28.03.2006 als unbegründet zurück (abgedruckt in DuD 2006, 313 f.). Die Speicherung der Personalausweisnummer sei »zur Erreichung des vertraglichen Zweckes«, die Durchführung sicherer Fußball-WM-Spiele, erforderlich, ja »unerlässlich« gewesen. Aufgeführt wird vom Gericht der Abgleich mit einer »Hooligan-Liste«, in der aber dummerweise keine Ausweisnummern gespeichert sind. Die Gefahrprognose sei über das übliche Maß hinausgegangen, vor allem »die Gefahr terroristischer Anschläge, insbesondere aus dem islamistischen Kreis«. Angesichts der öffentlichen Berichterstattung über den islamistischen Terrorismus bedurfte diese das Urteil tragende Prognose keiner weiteren Erläuterung.

Das Gericht erlaubte sich weitere beeindruckende Argumente. Es begründete nicht, weshalb die Ausweisnummer zur Gefahrenabwehr geeignet ist, sondern nur, dass »die weiteren gespeicherten Daten hierzu nicht geeignet sind«. Das vorgetragene Erwägung fällt in sich zusammen, wenn das gesamte Personalisierungskonzept untauglich war, so wie dieses sich auch nachträglich erwies.

Nicht unerwähnt lassen wollte das Amtsgericht »das Ansehen Deutschlands«, ohne erkennen zu lassen, was das mit den Daten des Klägers zu tun hat. Nicht ausdrücklich erwähnen woll-

te das Amtsgericht wohl, dass das Ansehen von Deutschland und des DFB dadurch gelitten hätte, wenn es korrekt die Rechtswidrigkeit der Personalisierung mit der Ausweisnummer festgestellt hätte. Der politische Schaden wäre doch zu groß gewesen!

Verblüffend ist, dass das Amtsgericht die zwei wesentlichen Regelungen, nach denen die Klage zu beurteilen war, nicht einmal zitierte, geschweige denn sauber rechtlich prüfte: Weder die oben genannte Regelung im PersAuswG noch die Regelung zur Rechtfertigung einer Datenspeicherung (§ 28 Abs. 1 Nr. 1 BDSG) wurden erwähnt, wohl in der richtigen Vermutung, dadurch würde die Entscheidung noch anfechtbarer, als sie ohnehin ist. Sowohl der Kläger wie auch der beklagte DFB hatten sich mit diesen gesetzlichen Regelungen ausführlich auseinandergesetzt. Es muss daher Vorsatz gewesen sein, dass das Gericht eine saubere juristische Argumentation unterließ. Es ging ja um Höheres: »Der eher als gering einzuschätzende Eingriff in das Selbstbestimmungsrecht des einzelnen hinsichtlich seiner Daten ist im Bezug auf den Vertragszweck und den legitimen Sicherheitsinteressen auch der Gesellschaft in Deutschland und des Staates Bundesrepublik als gerechtfertigt anzusehen« (alle wörtliche Zitate stammen aus dem Urteil des Amtsgerichtes; grammatikalische Fehler stehen so im Original).

4. Von der Wertigkeit des Datenschutzes

In einem ist dem Amtsgericht zuzustimmen: Die Speicherung der einen einzelnen Ausweisnummer war eher marginal; auch wenn sie ein Eingriff in das Recht auf informationelle Selbstbestimmung ist. Die Speicherung von Hunderttausenden von Ausweisnummern ist dagegen nicht mehr trivial. Gegen die Zigtausendfache Datenspeicherung gab es aber keine Klagemöglichkeit. Und genau diese Speicherung erfolgte und sie stand, indirekt, vor Gericht – für alle Beteiligten. Über den Zweck des Verbotes im PersAuswG konnte sich das Amtsgericht nicht auslassen, weil es dieses Gesetz bewusst ignorierte. Wenn es sich hierzu ausgelassen hätte, hätte es sich mit dem verfassungsrechtlichen Verbot von Personenkennzeichen (PKZ) auseinandersetzen können, auch damit, dass solche PKZ im Nazi- und im Stasi-Deutschland die Bevölkerungskontrolle erleichterten, und dass genau die DFB-Nutzung – auf zugegeben niedrigem Niveau – eine Verwendung der Nummer als PKZ darstellte. Das Gericht hätte sich auseinandersetzen können, hat es aber nicht wollen.

Das Urteil erging ja nur von einem Amtsgericht – könnte man sagen. Richtig ist, dass die Rationalität von Entscheidungen des Bundesverfassungsgerichtes regelmäßig erheblich höher ist. Doch es sind die Amtsgerichte, mit denen wir es im Alltag zu tun haben, auch wenn es um Datenschutz und um Sport geht. Und diese sollten unabhängig sein. Die Unabhängigkeit der Justiz besteht nicht schon, wenn nach erfolglosen Klagen in mehreren Instanzen die Chance besteht, vom Bundesverfassungsgericht auf eine Verfassungsbeschwerde hin eine unabhängige Entscheidung zu erhalten. Mit einer solchen hat das Urteil des Amtsgerichtes selbst bei wohlwollender Betrachtung wenig gemein. Nicht, dass das Gericht vom DFB gekauft gewesen, oder vom Bundesinnenministerium unter Druck gesetzt worden wäre. Dafür gibt es keine Hinweise. Dessen bedarf es auch nicht, wenn die öffentlichen Anreize bzw. Druckverhältnisse stark genug sind. Und dies war der Fall bei dieser Fußball-WM, an der sich auch noch ein halbes Jahr später in Jahresrückblicken auf 2006 die Bundeskanzlerin, die Medien und gemeine fernsehinterviewte Deutsche gefühlsberauschen ließen. Was spielt es da noch eine Rolle, dass es ein Personalausweisgesetz und andere Vorschriften gibt, oder dass es Gesetze der Logik und des rationalen Diskurses gibt.

5. Ein Lehrstück

Das ist das Erschreckende an dem unscheinbaren Urteil des Amtsgerichtes Frankfurt am Main: Es ist ein beredtes Zeugnis dafür, dass Justizia eine gefühlsschwankende Genossin ist, wenn es etwa um das Verhältnis von Staatsraison und Sport zu Grundrechtsschutz und informationeller Selbstbestimmung geht. Das Urteil ist auch ein Lehrstück, nicht nur dessen Ergebnis und Begründung, sondern der Weg dorthin. Es ist ein Lehrstück über die Kohabitation von Sport und etablierter Politik, über die Wertigkeit des Datenschutzes, wenn es um Höheres geht, nämlich wenn die Welt zu Gast bei Freunden ist, über die kollektive Bereitschaft, über Gesetze hinwegzusehen, wenn Sicherheit die Welt bestimmt (vgl. Weichert, digma 2.2006, 70 ff. = Forum Wissenschaft 2/2006, 10 ff. = www.daten schutzzentrum.de/polizei/weichert_ wm.htm).

Es ist ein ermutigendes Lehrstück, dass eine Demokratie des Widerspruchs gegen Autoritäten bedarf. Dies gilt erst recht, wenn es der Autoritäten viele sind: ein Fußballbund mit seinem Sicherheitskonzept, ein Bundesinnenministerium mit seiner Absegnung bzw. seiner Mitverantwortung für diese Konzept, ein Gericht ohne Blick für das Gesetz... Insofern können wir froh sein, dass es einen Fußballfan aus Dresden gab, der sich hierüber beklagte. Auch wenn er im konkreten Verfahren unterlag, könnte ihm die Geschichte dadurch Recht geben, dass beim nächsten Sportgroßereignis auf die Personalisierung der Tickets verzichtet wird.

Stellungnahme der DVD zur geplanten Änderung des Passgesetzes

Der Innenausschuss des Deutschen Bundestages hat sich am 23.4.2007 in einer Anhörung mit der Einführung von Reisepässen mit digitalisiertem Fingerabdruck in RFID-Chips und weiteren Vorschlägen zur Änderung des Pass- und Personalausweisrechts befasst. Dabei wurde u.a. auch über die Möglichkeit debattiert, zukünftig Passfotos durch die Polizei bei den Passbehörden online abrufen zu lassen. In der nachfolgenden Diskussion vermochte BKA-Präsident Jörg Ziercke viele Abgeordnete nicht davon zu überzeugen, dass die Zahl der bekannt gewordenen Manipulationen an deutschen Reisepässen tatsächlich den aufgerüsteten ePass notwendig macht. Debattiert wurde außerdem die technische Möglichkeit, ePässe unbemerkt auszulesen oder zu manipulieren. Bundesinnenminister Schäuble und der Bundesrat gehen inzwischen mit der Forderung, Lichtbilder und Fingerabdrücke zentral zu speichern und für die Strafverfolgung zu verwenden, weit über den dem Parlament vorliegenden Gesetzentwurf hinaus.

An der Anhörung nahmen als Sachverständige teil: Prof. Busch, Fraunhofer-Institut Darmstadt; Lukas Grundwald, DN- Systems GmbH Hildesheim (zum Clonen und softwaremässigen Manipulieren an ePässen), Sönke Hilbrans, DVD e.V. Bonn; Peter Schaar, BfDI; Dr. Schabhüser, BSI Bonn; Prof. Pfitzmann, TU Dresden; Jörk Ziercke, BKA Wiesbaden. Das Protokoll wird öffentlich zugänglich gemacht werden.

Bonn, den 19. April 2007

Stellungnahme

anlässlich der öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages am 23. April 2007 zu dem Gesetzentwurf der Bundesregierung für ein Gesetz zur Änderung des Passgesetzes und weiterer Vorschriften, BT-Drs. 16/4138, 14/4456, u.a.

I. Zu dem Gesetzentwurf der Bundesregierung, BT- Drs. 16/4138 vom 29.1.2007:

1. Die Speicherung von Fingerabdrücken in Reisepässen ist, ohne dass der Deutsche Bundestag und die Öffentlichkeit in angemessenem Umfang beteiligt worden wären, kraft Verordnung (EG) Nr. 2252/2004 angeordnet. Ebenso wie die Vorratsspeicherung von Telekommunikationsverbindungsdaten kommt die Verpflichtung nach der Verordnung nicht plötzlich und unverhofft über die Bevölkerung, sondern sie wurde unter Mitwirkung der Bundesregierung entwickelt. Einmal mehr zeigt sich darin auch im Bereich der inneren Sicherheit ein erschreckendes Demokratiedefizit in der Europäischen Union, welches in der Praxis nicht durch die nationalen Parlamente ausgeglichen werden kann.

2. Für die biometrische Ausrüstung deutscher Reisepässe ist ein praktisches Bedürfnis nicht nachgewiesen, so dass sich die informationellen Zumutungen, die mit der Erhebung und Speicherung biometrischer Daten im Passwesen verbunden sind, nicht auf triftige Gründe stützen können. Deutsche Reisepässe zählen nach dem Bekunden der Bundesregierung schon heute im weltweiten Vergleich zu den Spitzenprodukten. Demgegenüber bleibt eine Darstellung und Analyse der tatsächlichen Gefährdung durch ver- oder gefälschte deutsche Reisepässe auch in der Begründung der Bundesregierung zum Gesetzentwurf aus. Zahl und Art der ermittelten Fälle von (Ver-) Fälschungen deutscher Pässe bleiben ebenso im Dunkeln wie die bekannten Fehlerquellen bei der Erkennung von Fälschungen durch die Vollzugsbeamten. Angesichts des hohen Qualitätsstandards deutscher Reisepässe spricht vieles dafür, dass es vor allem ausländische Dokumente und allenfalls deutsche Ausweisersatzpapiere (soweit sie weiterhin ohne hochwertige technische Ausstattung und mit nur sehr primitiven biometrischen Merkmalen auskommen) sind, die ge- oder verfälscht Verwendung finden. Eine Evaluation des ePasses, wie sie der Bundesbeauftragte für Datenschutz und Informationsfreiheit zu Recht fordert, hat bislang keine Vergleichsdatenbasis, und der Erfolg des ePasses wird weitgehend spekulativ bleiben.

Der ePass ermöglicht die Erfassung und Speicherung biometrischer Daten von EU- BürgerInnen durch ausländische Staaten, ohne dass die Betroffenen oder die Mitgliedstaaten der Europäischen Union dagegen eine Handhabe hätten. Die Speicherung von Templates an Stelle von Echtdaten hätte demgegenüber die Nutzung von biometrischen Daten zu nicht gewünschten Zwecken wesentlich erschwert und sich als die datensparsamere Lösung erwiesen.

Auch die Festlegung auf die RFID-Technik löst Bedenken aus. Denn sie liefert die InhaberInnen von Reisepässen dem Risiko der unbemerkten Erfassung und Speicherung personenbezogener Daten, einschließlich biometrischer Daten, durch Dritte aus. Ungeachtet der getroffenen Sicherheitsmaßnahmen sind Lesevorgänge über die Luftschnittstelle leichter angreifbar als Lösungen, die einen direkten Kontakt mit dem in den Pass eingebrachten Chip erfordern. Die rasante technische Entwicklung und Verbreitung dieser Technik wird die Datensicherheit von ePässen in Zukunft zunehmend gefährden und im besten Falle in immer kürzeren Abständen Gegenmaßnahmen von staatlicher Seite erfordern, wenn nicht neue Sicherheitslücken auftreten sollen. Demgegenüber werden Fehler im gespeicherten Datensatz und bei seiner Übertragung in ein Lesegerät zukünftig jeder Stelle, die Zugriff auf diese Daten hat, vermeidbaren Anlass zu Zweifeln an der Identität der Betroffenen bieten.

Der Gesetzentwurf kommt auch mit der Befugnis für Beförderungsunternehmer nach § 18 Abs. 4 neu PassG ohne Not den von der Bundesrepublik nicht gewünschten Interessen ausländischer Bedarfsträger entgegen: anstatt die Vorabübermittlung von Passagierdaten mit den gegebenen Mitteln politisch einzudämmen, reagiert die Bundesregierung auf diese von einigen Drittstaaten geforderte Übermittlung mit einer spezielle Ermächtigung von

inländischen Beförderungsunternehmen. Eine substantielle Erleichterung für die Unternehmen besteht dabei nur bezüglich eines kleinen Teils der in der maschinenlesbaren Zone abgelegten Daten, da die Unternehmen von den Daten nach § 4 Abs. 2 Pass die Personalien der Flugpassagiere auch zu eigenen Zwecken – weiterhin konventionell – erheben und zur Vermeidung von ausländerrechtlichen Haftungsrisiken auch die Gültigkeit des Reisedokuments prüfen müssen. Spürbare Erleichterungen ergeben sich mithin lediglich im Umfang von etwa 22 Zeichen.

3. Bleibt die Entscheidung für einen ePass mit biometrischen Daten und RFID-Technik im Ergebnis sowohl praktisch als auch datenschutzpolitisch eine Fehlentscheidung ohne öffentlichen Rückhalt, kann dagegen ein anderer Effekt der biometrischen Aufrüstung von Identitätsdokumenten schon heute am Gesetzentwurf abgelesen werden: Wo qualitativ hochwertige Daten erfasst werden, wecken sie das Interesse der Sicherheitsbehörden an der Zweckentfremdung gespeicherter Daten, und dieses wird regelmäßig auch vom Gesetzgeber befriedigt. Dass rechtliche Schranken der Nutzung von Daten zu polizeilichen und nachrichtendienstlichen Zwecken sich einer fortwährenden Erosion ausgesetzt sehen, kann ohne Weiteres an der Sicherheitsgesetzgebung der letzten Jahre abgelesen werden. Nicht zu Unrecht wird diese Vorgehensweise als »Salamitaktik« bezeichnet.

Der Gesetzentwurf zur Passgesetznovelle treibt nunmehr die Nutzung von Lichtbildern in den Pass- und Personalausweisregistern durch Sicherheitsbehörden voran: Obwohl das Pass- und das Personalausweisregister unbestritten keine Auskunftsdateien für außerpassrechtliche Zwecke sind (etwa § 21 Abs. 3 PassG), werden sie schon heute routinemäßig als Refenzdatenbanken für die Identifizierung namentlich bekannter deutscher Staatsangehöriger herangezogen. Dieser Praxis überwindet den datenschutzrechtlichen Grundsatz der Zweckbindung personenbezogener Daten und ist schon im Hinblick auf die Subsidiarität der Registeranfrage (§§ 22 Abs. 2 Nr. 3 PassG, 2b Abs. 2 PersonalausweisG) rechtswidrig. Der Gesetzentwurf vollzieht mit dem Online-Abruf aus den Registern (§ 22a Abs. 2 S. 1 neu PassG, 2c Abs. 2 neu PersonalausweisG) den Übergang zur allgemeinen Zugriffsberechtigung für – zunächst – bestimmte ordnungsbehördliche Zwecke. Darin liegt nicht nur eine technische Vereinfachung: Der Online-Zugriff ermöglicht bei vorhandener technischer Infrastruktur in weit größerem Ausmaß als heute die Nutzung der bei den Registerbehörden bereits nahezu flächendeckend vorhandenen Lichtbilder der deutschen Wohnbevölkerung. Das Pass- und Personalausweisrecht beschränkt den Abruf und die Nutzung dieser Daten ebenso wenig auf die Betroffenen im Ordnungswidrigkeitenverfahren (in Abgrenzung zu Dritten) wie die in den §§ 22 Abs. 1, 2a Abs. 1 PersonalausweisG in Bezug genommenen Gesetze und Verordnungen. Dass für die rechtliche Erlaubnis zum Online-Abruf ein zwingendes öffentliches Bedürfnis bestehen soll, kann dabei nicht überzeugen: die Überlastung der Ordnungswidrigkeitenbehörden ist kein Anlass für die Einführung einer datenschutzkritischen Infrastruktur, und Alternativen – etwa die Aufhebung der Privilegierung von Verkehrsordnungswidrigkeiten durch eine Verlängerung der bislang außergewöhnlich kurze Verjährungszeit von drei Monaten – sind offenkundig nicht erwogen worden.

Die Zukunft des in dem Gesetzentwurf der Bundesregierung versprochenen Verbots einer bundesweiten biometrischen Datenbank (§ 4 Abs. 3 S. 3 neu PassG, vergl. auch Art. 4 Abs. 3 VO (EG) Nr. 2252/2004) dürfte im Hinblick auf Lichtbilder in der Sache kurz sein: die Kapazität zum Online-Abruf lässt es perspektivisch genügen, durch geeignete technische Ausstattung der abrufenden Stellen und Zugriff etwa auf meldebehördliche Daten auch dezentrale Passregister als Ermittlungsinstrumente für sicherheitsbehördliche Zwecke zu verwenden.

Die Lebensdauer der Beschränkung des Online-Abrufs auf die Verfolgung von Verkehrsordnungswidrigkeiten (§ 22a Abs.2 neu PassG) ist voraussichtlich sogar kürzer als das Gesetzgebungsverfahren: die Bundesregierung hat in ihrer Gegenäußerung zur Stellungnahme des Bundesrates (BT- Drs. 16/4456, dort Nr. 6.) bereits dem Online-Abruf von Lichtbildern zur Verfolgung von Straftaten zugestimmt.

II. Zu der Stellungnahme des Bundesrates und der Antwort der Bundesregierung, BT- Drs. 16/4456 vom 28.2.2007:

Der Bundesrat führt in seiner Stellungnahme die absehbare Zukunft von Passdaten vor. Diese soll, ganz im Sinne der Erosion von Verwendungsschranken gegenüber sicherheitsbehördlichen Zwecken, bestimmt sein von dem Wegfall der heute noch in das PassG eingeschriebenen Zweckbindungen.

In der Sache laufen die Forderungen des Bundesrates zu § 16a S. 2 neu PassG (Abgleich biometrischer Daten im ePass mit vorhandenen erkennungsdienstlichen Daten) und zu den §§ 22a Abs. 2 neu PassG, 2c Abs. 2 PersonalausweisG (Online-Abruf sämtlicher Registerdaten insbesondere durch Strafverfolgungsbehörden) auf die weitgehende Nutzung von Passdaten zu polizeilichen Zwecken hinaus. Der Sinn des ePasses – Fälschungssicherheit – und des Passregisters – Vollzug des Passgesetzes – werden unter Aufgabe des verfassungsrechtlich unverfügbaren Grundsatzes der Zweckbindung und des Verbotes der Datenerhebung und –speicherung »auf Vorrat« zu noch unbestimmten Zwecken in ihr Gegenteil verkehrt. Von den Vorschlägen des Bundesrates ist es nur ein kleiner Schritt zur Integration der Pass- und Personalausweisregister und des Systems biometrischer Ausweise in eine umfassende Infrastruktur sicherheitsbehördlicher Datenbanken.

Mit den Erfahrungen der vergangenen Jahre ist es abzusehen, dass der Deutsche Bundestag sich damit in nicht allzu ferner Zukunft ebenso wird auseinanderzusetzen haben, ebenso wie mit der Forderung, die heute noch einer strengen Zweckbindung unterliegenden Daten der LKW-Maut zu Hilfsmitteln der Sicherheitsbehörden werden zu lassen, wie es die Melderegister, das Kraftfahrzeugregister, die Bestandsdaten der Geldinstitute und der Telekommunikationsanbieter oder das Ausländerzentralregister schon standardmäßig heute sind.

Dieser Entwicklung gilt es, im Interesse einer freiheitlichen Gesellschaftsordnung, wie sie das Grundgesetz fordert, entgegenzutreten. Denn es wäre mit einer solchen Gesellschaftsordnung nicht vereinbar, wenn die Datenspuren alltäglicher und unvermeidlicher Lebensäußerungen dauerhaft und leichtgängig zu Instrumenten der Verdachtsgewinnung und Kontrolle würden.

Sönke Hilbrans
Rechtsanwalt und Fachanwalt für Strafrecht, Berlin
Vorsitzender der Deutschen Vereinigung für Datenschutz e.V., Bonn

Datenschutznachrichten

Tourismus-Nachrichten

Bund

Unerklärliche Spuren bei der Flugbuchung

Der Evangelische Pressedienst (epd) berichtet von einem Kunden, der im Herbst 2006 im Internet beim Reisevermarkter Opodo einen Flug in die USA buchte. Die Rechnung kam erst nach mehrfacher Aufforderung. Als sie dann kam, wunderte sich der Kunde, da in der Adressangabe über seinem Namen der Titel einer Bundeswehrkameradschaft auftauchte: »Marineoffiziercrew VII/76«. Tatsächlich hatte der Kunde als junger Leutnant mit dem Einstellungsjahrgang 1976, also vor 30 Jahren, dieser Marinecrew angehört. Es ist völlig unklar, woher Opodo von der Bundeswehrvergangenheit ihres Kunden wusste. Merkwürdig war zudem, dass hinter Postleitzahl und Ortsangabe im Adressfeld von Opodo der richtige Stadtteil aufgeführt wurde, obwohl der Kunde diese Angabe bei der Online-Buchung nicht gemacht hatte.

Der Reisende wandte sich an Opodo. Als man dort den Buchungsvorgang aufrief, tauchte keine »Marineoffiziercrew VII/76« auf. Servicemanager Gunter Wakulat von Opodo kann sich das Ganze nicht erklären, der Vorgang sei »ominös und mysteriös«. Seine Mitarbeitenden hätten »Stein und Bein geschworen«, dass sie den Kunden nicht kennen und die Adresse manuell nicht verändert hätten. Die zuständigen Landesbeautragten für Datenschutz wurden eingeschaltet. Ein Verdacht besteht darin, dass den US-Behörden beim Abgleich mit deren Sicherheitsdatenbanken der Kunde aufgefallen ist und diese Sicherheitsbedenken in die Kundendatenbank von Opodo, eine englische Firma gelangt ist. Denn schon vor dem Flug sind die Flugunternehmen verpflichtet 34 Angaben zu ihren Kunden, den sog Passenger Name Record an die US-Behörden zu liefern, damit dort etwaige Terrorismusgefahren präventiv festgestellt werden können. Unklar ist aber, wie die Daten zu Opodo gelangt sind, da die Meldung an die USA durch die Fluglinien erfolgt, nicht durch die buchenden Reiseunternehmen (Lilienthal, epd 21.12.2006).

Flugticket und Ausweis – identischer Name spart Ärger

Bei einer Flugbuchung sollten Reisende darauf achten, dass der Name auf dem Ticket identisch mit den Angaben im Reisepass oder Personalausweis ist. Kurzformen oder Spitznamen sollten – so der Ratschlag von Jan Bärwalde von der Lufthansa – durch den offiziellen Vornamen ersetzt werden. Aus Kati, Susi oder Gabi sollten – entsprechend dem Eintrag im Ausweis – wieder Katharina, Susanne und Gabriele gemacht werden. Anderenfalls könne es insbesondere bei Flügen in den Nahen Osten, in die USA und nach Großbritannien beim Einchecken oder der Passkontrolle zu Problemen kommen. Unter Umständen müssten Urlauber den Flug dann unter Zahlung einer Gebühr umbuchen, oder die Einreise werde ihnen möglicherweise sogar ganz verweigert (Kieler Nachrichten 13.01.2007, S. IV).

Hotelüberwachung – eine große Ungewisse

Auf dem 23. Chaos Communication Congress in Berlin am 27.12.2006 präsentierte der Coburger Sicherheitsberater Manfred Fink ein detailliertes Bild über den Stand staatlicher und privater Überwachung, die auch vor Hotelräumen nicht halt mache: »Die Frage muss lauten: Sind wir paranoid genug?« Er empfahl allen, die in Hotelzimmern Wert auf Privatsphäre legen, »kritische Geräte« wie Telefone, Fernsehgeräte oder Radiowecker zu entfernen. Ein Auge solle man auch auf die Schächte für die Klimaanlage haben, da dahinter Kameras versteckt sein könnten. Es gebe gerade in Luxusherbergen zahlreiche »verborgene Infrastrukturen«. Er empfahl, »einfach mal gegen die Decke zu drücken«. Der Wanzenjäger hatte zum Vortrag eine Kachel mit dahinter installiertem Mini-Elektroauge mitgebracht.

Hotelzimmer gehören lauf Fink »zu den unsichersten Orten überhaupt«, was die Vertraulichkeit von Kommunikation anbelangt. Sie böten Informationsbeschaffern ein leichtes Spiel. In einer fremden Umgebung sei der Aufwand groß, Abhörsicherheit herzustellen. Er riet davon ab, in Hotels Telekommunikationsanlagen ohne vertrauenswürdige Verschlüsselungstechniken zu benutzen und öffentliche WLAN-Netze in Anspruch zu nehmen. Generell sei es hilfreich, nicht alle Dinge bei einem Telefonat im Klartext zu benennen. Bei Emails sollten vertrauliche Informationen mit Hilfe von Steganografie im Datenwust etwa eines Bildanhangs versteckt werden. Faxe sollten handschriftlich diagonal beschrieben werden, um die OCR-Scansoftware der Lauscher auszutricksen.

Dass der Aufwand bei Bedarf angemessen sei, illustrierte Fink anhand von Medienberichten etwa über die audiovisuelle Überwachung im Hotel »Neptun« in Warnemünde und anderen von der Stasi unterwanderten Absteigen im ehemaligen Osten. 1997 sei aber auch aufgeflogen, dass im Marriott-Hotel in Wien in der Nähe des OPEC-Gebäudes drei Luxussuiten mit professionell ferngesteuerten Raumwanzen für Langwellenfunk ausgerüstet waren. Im Verdacht, die Mikros installiert zu haben, geriet damals die National Security Agency (NSA), der technische Geheimdienst der USA. Als Überwachungstrend machte Fink das Einschleusen präparierter Akkus in Mobiltelefone aus. Dazu reiche es aus, das Handy kurzzeitig unbeaufsichtigt zu lassen. In seiner Firma seien beim Röntgen mit hochauflösenden Digitalsystemen mehrere hundert Geräte mit Wanzen-Akkus entdeckt worden. »Mach Sie Kerben

oder Kratzer rein«, empfahl er. Er schätzte die Zahl der Geheimdienstler und Strafverfolger, die sich auf derlei Abhöraktionen spezialisiert hätten, auf »hoch dreistellig« (www.heise.de 28.12.2006).

USA

Datenschutzverstoß bei Flugdatenauswertung eingeräumt

Das US-amerikanische Ministerium für innere Sicherheit (Department of Homeland Security – DHS) räumte ein, dass während der Testphase für das Programm Secure Flight von der Transportation Security Administration (TSA) des Ministeriums vom Herbst 2004 bis Frühjahr 2005 mehr Daten gesammelt wurden, als im Gesetzblatt erlaubt. Dieser behördliche Datenschutzverstoß ergibt sich aus einem Bericht, den das DHS aktuell vorgelegt hat. Bei früherer Gelegenheit hatte der US-Rechnungshof derartige Bedenken geäußert, wodurch der Bericht initiiert wurde. In diesem heißt es, die TSA hatte in ihrer gesetzlichen vorgeschriebenen Ankündigung versichert, keine Daten aus »kommerziellen Quellen« zu sammeln, speichern oder nutzen.

Aus der abschließenden Mitteilung der Behörde konnte jedoch geschlossen werden, dass das Gegenteil der Fall war. Als Ursache für die Diskrepanz wird in dem Bericht mitgeteilt, dass die Datenschutzbestimmungen (Privacy Notices) verfasst wurden, nachdem das Programm komplett ausgearbeitet war. Derlei Verstöße brächten Programme wie »Secure Flight« in Verruf. Secure Flight war Ende 2004 von der US-Regierung als Ersatz für das gescheiterte Flugpassagierdatenbank-Projekt CAPPS II eingeführt worden. Mit ihm will man potenzielle Flugzeugentführer über Passagierdatenanalysen mit Data-Mining-Techniken schon vor dem Einchecken am Flughafen herausfiltern. Das Programm war Ende 2006 schon dadurch ins Zwielicht geraten, dass zehntausende Flugpassagiere fälschlicherweise als Terrorverdächtige gelistet wurden (www.heise.de 10.01.2007).

Deutsche Datenschutznachrichten

Bund

Bundes-Trojaner – bald gesetzlich geregelt?

I. Die Geschichte der Debatte

Mit der Entscheidung des Bundesgerichtshofes vom 31.01.2007, in der festgestellt wurde, dass es für heimliche Online-Durchsuchungen durch Strafverfolgungsbehörden an einer gesetzlichen Grundlage fehlt (s.u. S. 38), hatte die Diskussion über den Bundes-Trojaner – das staatliche Computer-Hacking – einen vorläufigen Höhepunkt erreicht.

Zuvor hatte sich das Bundesministerium des Innern (BMI) von der rotschwarzen Bundestagsmehrheit Gelder für die Entwicklung spezieller Hackersoftware genehmigen lassen. Das BMI betreibt das Projekt offensichtlich schon des Längeren. Nur über Umwege erfuhren die Parlamentarier hiervon: Die Haushälter wunderten sich über zwei Personalstellen, 225.000 Euro Sachkosten und 200.000 Euro einmalige Investitionskosten für einschlägige neue Hardware, die im Etat des BMI auftauchten. Im BMI-Programm zur Inneren Sicherheit war 2006 festgelegt worden: »Ein wichtiger Baustein im Kampf gegen den Terror ist die Fähigkeit, PCs durchsuchen zu können, ohne tatsächlich am Standort des Geräts zu sein.« Umgehend waren die neuen Begehrlichkeiten von DatenschützerInnen und ParlamentarierInnen wie z.B. von dem bündnisgrünen Wolfgang Wieland kritisiert worden.

Ob und in welchem Umfang von Strafverfolgern in Deutschland bisher Trojaner eingesetzt worden sind, kann nur schwer eindeutig beantwortet werden. Die c´t berichtet über einen Fall schon aus dem Jahr 1994, bei dem der BGH-Ermittlungsrichter den heimlichen Computerzugriff als Telekommunikationsüberwachung deklarierte. Dieser Fall war insofern untypisch, als der Zugriff auf den Computer mit Hilfe der Spuren direkt aus Ermittlungen zu einem Bombenanschlag erfolgte, nicht mit Hilfe eines Trojaners (Az. 1 BGs 625/95).

In der Presse ist von zwei weiteren Fällen die Rede. So genehmigte das Amtsgericht Bonn einen Cyber-Angriff auf Computer einer Phishing-Bande aus den USA, die Kreditkartennummern und Zugangsdaten von Internet-Nutzern ausspionierten. Gehackt wurden bei den Ermittlungen im Jahr 2006 allerdings nur zwischengeschaltete Computer, sog. Anonymisierungs-Rechner, nicht private Computer. Im März 2006 hatte die Generalbundesanwältin das Bundeskriminalamt gebeten, die technischen Voraussetzungen für das staatliche Hacking zu schaffen und dabei erwähnt, dass »dem Vernehmen nach verschiedene deutsche Sicherheitsbehörden bereits seit geraumer Zeit erfolgreich mit dem Instrument des heimlichen Abziehens von Daten auf fremden Computern« arbeiten. Bei diesen Sicherheitsbehörden sind offensichtlich Geheimdienste gemeint (s.u. S. 26f.). Das BMI gab auf eine Presseanfrage Ende 2006 beschwichtigend bekannt, dass das Bundeskriminalamt (BKA) solche Maßnahmen »nur in wenigen Fällen angewandt« habe.

II. Die politische Debatte

Nach dem Urteil des BGH-Senats forderte Bundesinnenminister Wolfgang Schäuble umgehend die zeitnahe Schaffung einer Rechtsgrundlage. Ins gleiche Horn stieß kurz darauf der Präsident des BKA, Jörg Ziercke. Die Polizei benötige die Online-Durchsuchung zur Bekämpfung des internationalen Terrorismus und der organisierten Kriminalität. Man müsse mit dem technischen Fortschritt Schritt halten, wenn »skrupellose Kriminelle« ins Internet auswichen und dort ihre kriminellen Handlungen vorbereiteten. Die Online-Durchsuchung sei »unerlässlich für die Strafverfolgung«.

Die Befürworter der heimlichen Online-Durchsuchung verweisen darauf, dass Verdächtige im Bereich des Terrorismus wie auch bei anderer Kriminalität das Internet zur Rekrutierung, Ausbildung, Planung und teilweise Aus-

führung von Straftaten nutzen, ohne dass sie hierbei angemessen beobachtet werden könnten.

BKA-Fahnder beteuerten immer wieder, die »aufwändige Technik« nur bei wirklich heiklen Verfahren zum Einsatz bringen zu wollen. BKA-Präsident Ziercke meinte: »99,9% der Menschen werden von dieser Maßnahme überhaupt nicht betroffen sein«. Weil das Bundesverfassungsgericht einen Kernbereich privater Lebensführung vom großen Lauschangriff ausgenommen habe, sei das Instrument des Abhörens praktisch unbrauchbar geworden: »Das darf mit der Online-Durchsuchung nicht passieren. Die Polizei muss mit dem technischen Fortschritt der Täter mithalten«.

Das bayerische Kabinett beauftragte Justizministerin Beate Merk und Innenminister Günther Beckstein (beide CSU), eine Rechtsgrundlage für heimliche Online-Durchsuchungen von PCs zu prüfen. Niedersachsen Innenminister Uwe Schünemann (CDU) forderte einen unbeschränkten Online-Zugriff auf Computer verdächtiger Personen. Heimliche Online-Durchsuchungen seien ein unerlässliches Instrument für die Strafverfolgung: »Wenn wir diese Methode nicht nutzen, hätten wir in der Strafverfolgung eine weltweite Lücke.«

Skeptisch äußerten sich dagegen SPD-PolitikerInnen. Bundesjustizministern Brigitte Zypries warnte vor Schnellschüssen, die in Karlsruhe keinen Bestand hätten. Die Behörden müssten erklären, warum sie Computer online durchsuchen müssten und nicht zu den gleichen Ergebnissen kämen, wenn sie physisch in eine Wohnung gingen und die Festplatte kopierten. Auch müsse genau geprüft werden, »inwieweit die Strafverfolgungsbehörden in den Kernbereich privater Lebensgestaltung eingreifen könnten und wie dem zu begegnen ist«. Der schleswig-holsteinische Innenminister Ralf Stegner (SPD) sowie der innenpolitische Sprecher der SPD-Bundestagsfraktion, Dieter Wiefelspütz, plädierten dafür, die gesetzlichen Hürden für Online-Durchsuchungen möglichst hoch zu setzen; der private Lebensbereich müsse dabei – so Wiefelspütz – ein »absolutes Tabu« bleiben. Der SPD-Abgeordnete Karsten Rudolph sprach von »staatlich organisiertem Hausfriedensbruch«. BKA-Präsident Ziercke zeigte sich im Rahmen der Debatte über der Warnung von Zypries vor »staatlichen Hackern« verärgert: Polizisten würden nicht zu kriminellen Hackern, wenn sie online durchsuchten. Das lasse sich »durch ein Gesetz eindeutig regeln«.

III. Die Technik

Entgegen der Darstellung mancher Strafverfolger ist das polizeiliche Hacken – je nach den vorhandenen Gegebenheiten – technisch relativ einfach. Durch eine unauffällige Email oder eine getarnte Internet-Seite installiert die Polizei ein Schnüffel-Programm auf dem Rechner des Verdächtigten. Ein solcher Trojaner versendet, wenn der Rechner online ist, die auf der Festplatte gespeicherten Daten an die Polizei. So ist es der Polizei grds. möglich, sämtliche Bits und Bytes, die auf der Festplatte gespeichert sind, zu erhalten. Moderne Betriebssysteme und Computeranwendungen sind inzwischen so komplex, dass sie kaum frei von Fehlern sein können. Diese werden dauernd mit Hilfe von Patches auszubügeln versucht. Die Lücken können aber nicht so schnell gefüllt werden wie die Angriffsmöglichkeiten bekannt werden. In dieser Zwischenzeit besteht die Möglichkeit für bösartige Cracker oder staatliche Strafverfolger, einen sog. Exploit zu schreiben, um über Ausnutzung der Lücke das Kommando über fremde Rechner zunehmen. Um auf einen privaten Rechner zu kommen, können sich die Ermittler auch an das Software-Unternehmen wenden und sich im Rahmen der Software-Aktualisierung auch den Trojaner mit aufspielen lassen.

Schadprogramme können per Spam-Email generell verbreitet werden, oder aber gezielt an bestimmte Email-Accounts. Online-Ermittler können sich im Prinzip all der Möglichkeiten bedienen, die auch kriminelle Hacker nutzen. Ob in einen Rechner eingebrochen werden kann, hängt von der Sorgfalt des Rechnerbetreibers und der von ihm verwendeten Software ab. So kann der Einbruch »kinderleicht« sein, unter Umständen aber auch »praktisch unmöglich«. Möglich ist es, mit Hilfe eines Trojaners einen Computer aus der Ferne komplett zu steuern incl. Einschalten der Webcam, akustische Wohnraumüberwachung per Mikrofon, Mithören von Internet-Telefonaten, Mitlesen von Chat und Email, Lifeübertragung von Webseitenabrufen und natürlich Kopieren des gesamten gespeicherten Datenbestandes.

Nach Pressemeldungen haben Schweizer Ermittler eine private Sicherheitsfirma, die ERA IT Solutions, damit beauftragt, eine Spionagesoftware zum Abhören von Internettelefonaten zu programmieren. Die Software soll weder von Antiviren-Programmen noch von Firewalls erkannt werden. Das Programm sendet Mitschnitte in kleinen Datenpaketen an einen Server.

Besonders problematisch ist, dass mit der Durchführung einer Online-Durchsuchung das Anlegen und Verändern von Dateien auf dem durchsuchten Computer verbunden ist. So können auch Beweismittel per Mausklick problemlos und spurenfrei auf dem infiltrierten Rechner angelegt oder manipuliert werden. Der Verdächtige hätte im Zweifel keine Chance, eine Manipulation auf seinem Computer nachzuweisen. Heimlich eingeschmuggelte kinderpornografische Bilder wären leicht dazu einzusetzen, eine missliebige Person effektiv mundtod zu machen. Umgekehrt kann sich ein Verdächtigter immer damit herausreden, dass die vorgefundenen Programme nicht von ihm stammten und ihm untergeschoben worden seien.

Virenscanner und Firewalls können einen sehr weitgehenden Schutz bieten. Doch eine sichere Abwehr eines Schnüffelangriffs ist kaum möglich. Kommerzielle Abwehrprogramme können den Nachteil haben, dass sie auf Wunsch von staatlichen Strafverfolgern gerade keinen Schutz vor deren Angriffswerkzeugen vorsehen. Ob ein Angriff stattfindet oder erfolgreich war, bekommt ein Überwachter u.U. nicht mit. Einen ziemlich sicheren Schutz vor dem staatlichen Ausspionieren gespeicherter Inhalte bietet die Verschlüsselung. Mit einer Container-Verschlüsselung ist es möglich sogar zu verbergen, dass überhaupt Inhalte – verschlüsselt – abgelegt worden sind.

IV. Die Argumente der Datenschützer

Der bayerische Datenschutzbeauftragte Karl Betzl hält heimliche Online-Durchsuchungen für einen freiheitlich-demokratischen Rechtsstaat unwürdig: »Die Festplatte eines Computers ist so etwas wie das Gedächtnis eines Menschen oder Unternehmens. Ein heimliches Ausforschen dringt tief in die Privatsphäre bzw. in die Geschäftsgeheimnisse ein. Wo bleiben da noch die letzten Reste eines ausforschungsfreien Raumes?« Betzl warnt vor immensen Scha-

densersatzansprüchen gegen den Staat, wenn z.B. anlässlich einer verdeckten Online-Untersuchung eines Unternehmens dessen EDV-System beschädigt wird oder Geschäftsgeheimnisse in die falschen Hände geraten: »Es ist unkontrollierbar, wie sich staatliche Ausforschungssoftware weiter verbreitet bzw. wie sie verbreitet wird und der Staat dürfte auch für Trittbrettfahrer mithaften, die die staatliche Ausforschungssoftware missbrauchen«.

Thüringens Datenschutzbeauftragter Harald Stauch bewertet das heimliche Ausspähen privater Rechner mit Hilfe eingeschleuster Programme als einen schwereren Eingriff als eine Telefonüberwachung. Stauch, der zuvor 16 Jahre CDU-Landtagsabgeordneter war, sprach nach seinem ersten Amtsjahr von einem »anderen Blick« auf den Konflikt zwischen Sicherheit und Freiheitsrechten: »Als Politiker haben sie mehr die Sicherheit im Blick. Aus unserer Sicht gibt es einen ausufernden Datenhunger des Staates. Spektakuläre Straftaten wie etwa Morde oder Kinderpornografie würden genutzt, um ohne öffentlichen Widerstand Grenzen auszuloten. Im Gegensatz zu Forderungen von Innenministern gehe es nicht darum, alles ›Menschenmögliche‹ zu tun, sondern alles »Rechtmäßige«.

Der Berliner Datenschutzbeauftragte Alexander Dix äußerte sich ähnlich kritisch: »Es ist widersinnig, dass Sicherheitsbehörden einerseits zu Recht Schutzmaßnahmen gegen den Einsatz von Spionageprogrammen durch Wirtschaftskriminelle fordern, andererseits aber genau diese Schadprogramme einsetzen wollen.« Da die Durchsuchung für die Betroffenen nicht kontrollierbar erfolge, gäbe es »keine technischen Schranken für die umfassende Ausforschung beliebiger Bürger. Online-Durchsuchungen schaden der inneren Sicherheit und sind verfassungswidrig.«

V. Volkes Stimme

Auf dem 10. Europäischen Polizeikongress am 16.02.2007 meinte der BKA-Präsident, 64% der Bevölkerung seien dafür, dass bei den Online-Durchsuchungen ein Kompromiss gefunden werde. 24% sagten, die Polizei solle diese Möglichkeit bekommen. Nur 11% seien völlig dagegen. Dabei beruft er sich offensichtlich auf eine Umfrage des Meinungsforschungsinstituts Infratest dimap im Auftrag des ARD-Morgenmagazins. TNS-Forschung führte am 06. und 07.02.2007 für den Spiegel eine Umfrage bei 1000 Personen durch zur Frage: »Halten Sie eine rechtliche Grundlage zur heimlichen Ausspähung von Privatcomputern durch die Polizei, etwa zur Bekämpfung von Kinderpornografie und Terrorismus, für sinnvoll?« 68% antworteten mit »Ja«; 28% mit »Nein« (PE MdB Montag&Wieland v. 05.02.2007; PM BayLfD 05.02.2007; Gebauer www.spiegel.de 05.02.2007; Dambeck www.spiegel.de 06.02.2007; www.spiegel.de 07.02.2007; www.heise.de 07.02.2007; Der Spiegel 7/2007, 22; Störing c´t 5/2007, 58 ff.; Bornhöft/Gebauer/Rosenbach Der Spiegel 7/2007, 42 ff.; www.heise.de 10.02.2007; www.heise.de 16.02.2007; SZ 17/18.02.2007, 6).

Bund

O2-Kundennummern im Internet

Die Telefonnummern von ca. 1000 KundInnen des Mobilfunkanbieters O2 sind im Internet veröffentlicht worden. Nach Bekanntwerden wurde »intensiv« geprüft, wie es dazu kommen konnte, meinte eine Sprecherin der Telefonica-Tochter. Betroffen waren KundInnen mit dem Tarif Surf&Email, denen wegen zu hoher Nutzung der Wap-Flatrate gekündigt worden war. Neben den Handy-Nummern befand sich ein Vermerk, ob aus Kulanz die Nutzung der Flatrate weiter erlaubt werde. Die Sprecherin bekräftigte, dass O2 den Datenschutz sehr ernst nehme. Über interne Ermittlungen solle der Mitarbeiter gefunden werden, der die Liste ins Netz gestellt habe (SZ 07.11.2006, 21).

Bund

Schufa löscht Bagatellforderungen früher

Seit Anfang 2007 zeigt sich die Schufa gegenüber säumigen SchuldnerInnen von geringen Beträgen nachsichtiger als bislang. Die Schufa Holding AG teilte am 11.01.2007 mit, dass seit Jahresbeginn Einträge über Forderungen von bis 1000 Euro unter bestimmten Voraussetzungen schon nach kurzer Zeit wieder gelöscht werden, wenn der Betrag von der SchuldnerIn zwischenzeitlich beglichen wurde. Bisher waren derartige Forderungen nach Begleichung der Schulden noch drei Jahre zum Jahresende in der »Kreditbiografie« der Person notiert. Voraussetzungen für die nunmehr mögliche kurzfristige Löschung sind, dass der Eintrag erstmals nach dem 01.01.2007 gemeldet, die Forderung innerhalb eines Monats beglichen sowie der Ausgleich vom Gläubiger der Schufa mitgeteilt wird. Darüber hinaus darf es sich nicht um eine sog. titulierte Forderung wie etwa einen Vollstreckungsbescheid handeln (SZ 12.01.2007, 17).

Bund

Eine halbe Million Luftverkehrs-Zuverlässigkeitsprüfungen

Seit dem Inkrafttreten des Luftsicherheitsgesetzes am 15.01.2005 bis Dezember 2006 sind ca. 513.400 Zuverlässigkeitsprüfungen durchgeführt worden. Von der Ausdehnung der Zuverlässigkeitsprüfung sind erlaubnispflichtige LuftfahrerInnen von Flugzeugen, Drehflüglern, Luftschiffen, Motorseglern und entsprechende FlugschülerInnen, PrivatpilotInnen und außerhalb von Luftfahrtunternehmen tätige BerufspilotInnen erfasst. Gemäß den vorliegenden Ländermeldungen sind davon 47.200 Personen von der Zuverlässigkeitsüberprüfung betroffen. Nach Mitteilung der Länder und des Luftfahrtbundesamtes kam es bisher in 46 Fällen zu einer vorläufigen Entziehung bzw. zu einem Ruhen der Lizenz (hib 11.12.2006 Nr. 379, BT-Drs. 16/3413 u. 3166).

Bund

Merkel für mehr Überwachung trotz hoher Sicherheit

Anlässlich eines Gewerkschaftskongresses der Polizei am 13.11.2006 lobte die Bundeskanzlerin Angela Merkel in einem Video-Podcast die Erfolge der Sicherheitskräfte: »Wir leben in Deutschland in einem der sichersten Länder der Welt. Glücklicherweise ist die Kriminalitätsrate leicht rückläufig. Die Zahl der aufgeklärten Straftaten ist in den letzten Jahren leicht angestie-

gen. Und vor allen Dingen hatten wir ein Erlebnis in diesem Sommer: eine wunderschöne und eine sichere Weltmeisterschaft«. Ergänzend versicherte die Kanzlerin, dass dies natürlich nicht ausreiche, solange sich die Bürger subjektiv nicht sicher fühlten. Deshalb brauche man nicht nur wachsame Bürger mit Zivilcourage, sondern müsse auch Mittel wie die Videoüberwachung einsetzen, um sich u.a. vor rechtsextremistischen Straftaten zu schützen.

Gegen Bedrohungen wie den internationalen Terror reiche dies allein aber nicht, da müsse man völlig neue Wege gehen. Merkel lobt umstrittene Maßnahmen als probate Mittel zur Erhöhung der Sicherheit: zusätzliche Millioneninvestitionen, die gemeinsame Anti-Terror-Datei sowie die Nutzung der LKW-Mautdaten zur Verfolgung von Terroristen sollen Deutschland noch sicherer machen. Deutschland werde im ersten Halbjahr 2007 die EU-Präsidentschaft nutzen, um auf europäischer Ebene unter anderem die schon länger betriebene Stärkung von Europol voranzutreiben. »Wir tun alles, um die Innere Sicherheit in Deutschland und in Europa zu gewährleisten«. Zusammenfassend: Es läuft alles prima, aber dennoch benötigen wir mehr Überwachung (www.heise.de 12.11.2006).

Bund

»Mehr Demokratie« durch gläserne Politiker

Der Verein »Mehr Demokratie« hat ein Kommunikationsportal zu den Abgeordneten des Bundestages eingerichtet. Auf http://www.abgeodnetenwatch.de kann sich jede und jeder informieren, wie der Direktkandidat seines Wahlkreises heißt und wie sich die Abgeordneten bei Abstimmungen verhalten haben, zumindest soweit diese dokumentiert sind wie z.B. bei namentlichen Abstimmungen. Die Abgeordneten werden den jeweiligen Ausschüssen zugeordnet. Außerdem gibt es Kurzportraits mit Angaben zur Person. Außerdem besteht die Möglichkeit, dass BesucherInnen Fragen an die Abgeordneten stellen. Unklar ist aber, ob die PolitikerInnen die an sie weitergeleiteten Fragen beantworten werden (www.heise.de 27.12.2006).

Mehrere Länder

Gesundheitstests für Dreijährige

In Nordrhein-Westfalen (NRW) sollen nach einem Plan des Familienministers Armin Laschet (CDU) künftig Dreijährige vor der Aufnahme in einen Kindergarten auf ihre Gesundheit getestet werden: »Je früher wir Auffälligkeiten entdecken, desto früher können wir eingreifen und helfen.« Für eine bundesweite Umsetzung dieser Maßnahme setzte er sich anlässlich der Jugendminister-Sonderkonferenz der Länder am 24.11.2006 ein. Bei den neuen ärztlichen Eingangsuntersuchungen für Kindergartenkinder soll gezielt auf Anzeichen für Misshandlungen und Vernachlässigungen geachtet werden. Vorbild für die Tests sind die obligatorischen Gesundheitskontrollen für Schulanfänger. Das NRW-Programm enthält auch einen Prüfauftrag an alle Jugendämter. Deren Mitarbeiter sollen künftig bei unangemeldeten Hausbesuchen drogenabhängige Eltern auf ihre Erziehungsfähigkeit untersuchen.

Auch der saarländische Gesundheitsminister Josef Hecken will die bislang freiwilligen Vorsorgeuntersuchungen verpflichtend machen, selbst wenn die anderen Länder nicht mitziehen: »Ab dem ersten Quartal wird bei uns eine Screeningstelle überwachen, ob Eltern die Untersuchungen ihrer Kinder wahrnehmen. Wenn nicht, werden die Gesundheitsämter informiert.« Die bayerische Sozialministerin Christa Stewens (CSU) meinte, das Datenschutzgesetz müsse geändert werden, um die Daten der etwa fünf Prozent, die die derzeitig schon angebotenen Vorsorgeuntersuchungen nicht wahrnähmen, an die Jugendämter übermitteln zu können. Latschet auf NRW meint, für einen Alleingang der Länder fehlten die rechtlichen Voraussetzungen etwa für den Datenaustausch zwischen Krankenkassen und Gesundheitsämter. Auch die Sozialministerin Hessens Silke Lautenschläger (CDU) assistierte: »Die Länder haben keine Handhabe, die von den Kassen angebotenen Untersuchungen verpflichtend zu machen. Dafür ist Bundesrecht erforderlich.« Bundesfamilienministerin Ursula von der Leyen (CDU) lehnte dagegen Forderungen nach bundeseinheitlich vorgeschriebenen ärztlichen Pflichtuntersuchungen ab. Aus ihrer Sicht haben die Länder die Handhabe für solche Untersuchungen. Diese könnten sofort über den Gesundheitsdienst eingeführt werden (Der Spiegel 46/2006, 22; Eckförd. Ztg. 15.11.2006, fu 133; vgl. S. 36).

Bayern

Stoiber-Mitarbeiter wollte Privatsphäre von Parteigegnerin ausspitzeln

Kurz vor Weihnachten, am 19.12.2006 informierte die Fürther Landrätin und Mitglied im CSU-Landesvorstand Gabriele Pauli auf einer Vorstandssitzung die CSU-Spitze, dass der bayerische Ministerpräsident Edmund Stoiber sie bespitzeln lasse. Stoiber ging dort auf die Sache nicht ein und wiegelte ab: »So wichtig sind Sie nicht.« Nach Paulis Darstellung ging es in einem rund einstündigen Telefonat mit dem Wirtschaftsreferenten der Stadt Fürth Horst Müller ausschließlich um ihr Privatleben. Mit wem sie, die geschieden ist, verkehre. Ob sie vielleicht ein Alkoholproblem habe. Ob es nicht irgendetwas gäbe, was man ihr anhängen könne. Vor der Vorstandssitzung hatte Pauli mehrfach um einen persönlichen Termin mit Stoiber gebeten, war damit aber abgeblitzt.

Pauli war das einzige CSU-Vorstandsmitglied, das nach dem Rückzug Stoibers aus Berlin nach der Bundestagswahl im Oktober 2006 in einem Antrag auf dem CSU-Parteitag indirekt Stoibers Rückzug aus der Politik gefordert und über ein von ihr eingerichtetes Internetforum offen zur Diskussion über Stoiber eingeladen hatte. Der Büroleiter des Ministerpräsidenten Michael Höhenberger gab zunächst nur zu, dass er sich bei einem Parteifreund über die Stoiber-Kritikerin informiert habe, was diese gegen den Ministerpräsidenten habe. Erst nachdem der Gesprächspartner Müller die genauen Nachfragen zum Privatleben von Höhenberger bestätigte, nahm dieser die Verantwortung für die Aktion voll auf sich und erklärte seinen Rücktritt. Höhenberger hatte auch schon in der Vergangenheit in delikaten Angelegenheiten Stoiber dadurch entlastet, dass er Initiativen zu eigenen erklärte, von denen Stoiber nichts gewusst habe.

Nach Paulis Darstellungen betreibt die CSU-Spitze ein Spitzelsystem, »um Kritiker mundtot zu machen.« Seit Bekanntwerden der Aktion gegen sie hätten sich bei ihr weitere Mandatsträger

gemeldet, die Ähnliches erlebt hätten. Die Betroffenen fürchteten aber aus Furcht vor Repressalien die Öffentlichkeit. Dies wird von einem intimen Kenner der Partei bestätigt. »Es gibt eine Abteilung Desinformation, es gibt eine Abteilung Schmutz, und sie sind vereint in einer Person: Höhenberger.«

Nachdem er tagelang jede Stellungnahme verweigert hatte, äußerte sich Stoiber erstmals am Heiligabend. Höhenberger habe ihn über seine Telefonaktion »nicht informiert und ich hätte das nie zugelassen«. CSU-Generalsekretär Markus Söder forderte Pauli auf, sie solle »endlich aufhören, Unruhe in der CSU zu stiften«. CSU-Fraktionschef Joachim Herrmann wies Paulis Vorwurf eines parteiinternen Spitzelsystems als »ausgemachten Unsinn« zurück. Wie dem auch sei. Jedenfalls brachte diese Spitzel-Affäre das Fass zum Überlaufen. Der sich hierüber aufgestaute Unmut und die zunehmende Kritik an ihm veranlassten Edmund Stoiber Mitte Januar 2007, seinen Rücktritt als CSU-Vorsitzender oder bayerischer Ministerpräsident im darauf folgenden September anzukündigen (Fahrenholz/Stroh SZ 21.12.2006, 1, 3, 4; Ritzer/Przybilla SZ 27.12.2006, 5; Neukirch/Verbert Der Spiegel 1/2007, 30 f.).

Baden-Württemberg

Videoatlas von privaten Kameras für die Polizei

2006 hatte der Innenminister des Landes Baden-Württemberg Heribert Rech (CDU) angekündigt, dass die Polizei auch die »Überwachungskameras privater Betreiber« nutzen soll. Die überwiegende Zahl der Videokameras befinde sich in nichtöffentlichen Bereichen: »Die Polizei soll sich in einem Einkaufszentrum aufschalten können, wenn da etwas passiert. Und dann möchte ich wissen, wo im Umkreis des Tatortes andere Kameras stehen«. Auch bei großen Menschenansammlungen soll die Videoüberwachung möglich sein. Für die Polizei soll ein »Atlas« aller Videokameras erstellt werden. Außerdem soll es zu einer Kooperationsvereinbarung mit den Betreibern kommen. Als Grund für die Ausdehnung der Videoüberwachung gibt Rech die »Gefahr islamistischer Terroranschläge« an. Für die Erstellung der Übersicht und den Zugriff auf private Kameras müsste allerdings das Polizeigesetz geändert werden, was noch nicht geschehen ist.

Die Grünen im Landtag haben erfahren, dass vom Innenministerium bereits Betreiber privater Videoüberwachungsanlagen befragt wurden. Sie protestierten gegen dieses Vorgehen, für das jede rechtliche Grundlage fehle. Der innenpolitische Sprecher der Landtagsgrünen Uli Sckerl spricht von Rechs »Video-Phantasien«, die weit über die Beschlüsse der Innenministerkonferenz zur erweiterten Videoüberwachung hinausgingen: »In Baden-Württemberg will der Minister private Betreiber von Videokameras zum verlängerten Arm der Polizei machen, wo diese nicht tätig werden darf« (www.heise.de 17.02.2007).

Brandenburg

Gutachter halten Polizeigesetzentwurf für verfassungswidrig

Bei einer Anhörung zum Entwurf zur Neufassung des Brandenburger Polizeigesetzes am 16.11.2006 erklärte der Vorsitzende des Berliner Anwaltsvereins und Mitglied des Vorstands des Deutschen Anwaltsvereins (DAV) Ulrich Schellenberg: »Die im Entwurf enthaltenen Regelungen der präventiven Telekommunikations- und Wohnraumüberwachung sind schlicht verfassungswidrig. Die Voraussetzungen für die Tatbestände seien viel zu schwammig formuliert. Es werde eine Regelung aus Niedersachsen kopiert, die 2005 für verfassungswidrig erklärt worden sei. Auch der Branchenverband Bitkom kritisierte, der Entwurf entspräche nicht den Vorgaben des Bundesverfassungsgerichtes in den Urteilen zum niedersächsischen Polizeigesetz und zur Rasterfahndung. Der DAV protestierte gegen den erneuten Versuch, das besondere Vertrauensverhältnis zu Berufsgeheimnisträgern wie Anwälten, Ärzten und Geistlichen auszuhöhlen. Die im Entwurf enthaltenen Schutzvorschriften gegen das Abhören und für die weitere Verwendung der Daten seien nicht ausreichend. Für den Lauschangriff auf Telefon und Wohnung fehlen laut Schellenberg Regelungen, nach denen die Abhörmaßnahme nicht begonnen werden darf, wenn der Kernbereich privater Lebensführung erkennbar davon betroffen wäre. Er verwies zudem auf handwerkliche Fehler, z.B. auf einen Verweis zu einer Regelung des Strafgesetzbuches, die 2005 aufgehoben worden ist.

Der Landesverband des Bundes Deutscher Kriminalbeamter (BDK) begrüßte in Person des stellv. Landesvorsitzenden Gerd-Christian Treutler dagegen die vorgesehenen Änderungen im Großen und Ganzen, sieht aber unter den angekündigten Stellenkürzungen die Gefahr, dass die vorgesehene Ausweitung polizeilicher Befugnisse »zum bloßen Papiertiger« verkommt: »Was nutzen Befugnisse, wenn es kein Personal für ihre Umsetzung gibt. Unsere Forderung lautet: Befugnisse, Technik und Personal, nicht aber statt Personal«. Kernpunkte der Erweiterung, wie Video- und Telefonüberwachung zur Gefahrenabwehr seien nur mit einem entsprechenden Personalaufwand sinnvoll einsetzbar (www.heise.de 15.11.2006).

Bremen

Erstes bremisches Datenschutz-Audit

Die Entsorgung Nord GmbH (ENO) wurde für den datenschutzkonformen Einsatz ihrer Betriebsstättensoftware LEWIN erfolgreich nach der Bremischen Datenschutzauditverordnung zertifiziert. Auf dem für die Entsorgungswirtschaft konzipierten System werden sowohl Daten sämtlicher Bremer Hauseigentümer als auch sämtlicher ENO-MitarbeiterInnen gespeichert. Damit ist ENO das erste Unternehmen in Bremen, das ein Datenschutz-Gütesiegel verliehen bekommt. Durchgeführt wurde die Auditierung durch die datenschutz nord GmbH (PE datenschutz nord 19.01.2007).

Hessen

Kfz-Kennzeichen-Scanning gestartet

Nach umfangreichen Tests nehmen neun Kameras bei der hessischen Polizei den Dienst auf, mit denen Autokennzeichen automatisch erfasst und überprüft werden. Bei der Vorstellung des automatischen Kennzeichen-Lesesystems (ALKS) am 11.01.2007 in Frankfurt erklärte der hessische Innenminister Volker Bouffier (CDU), Ein-

satzschwerpunkt sei das Rhein-Main-Gebiet mit dem Frankfurter Kreuz als Knotenpunkt. Die insgesamt 300.000 Euro teuren Geräte würden zunächst nur mobil eingesetzt; ein Dauerbetrieb an einem festen Ort sei aber auch möglich. Hessen übernehme mit dieser Technik eine Vorreiterrolle; nur in Bayern gebe es Vergleichbares. Mit ALKS werden die Kennzeichen der vorbeifahrenden Fahrzeuge erfasst und mit dem Datenbestand des polizeilichen Fahndungscomputers INPOL verglichen. Ergibt der Datenabgleich einen »Treffer«, so werden Polizeikräfte in der Nähe alarmiert, um das Fahrzeug und seine Insassen zu kontrollieren

Die bisherigen Tests haben jedoch gezeigt, dass die Daten, die vom System ausgeworfen werden, fehlerhaft sein können. Nach Angaben von Polizeirat Bernd Ricker von der Hessischen Polizeischule waren bis zu 40% der gemeldeten Verdachtsfälle nicht zutreffend. Das liege v.a. daran, dass das System sehr ähnliche Kennzeichen aus technischen Gründen nicht auseinander halten könne. Deshalb soll künftig ein Polizist die gelieferten Ergebnisse manuell kontrollieren, bevor es zu einem Zugriff kommt. Die Daten nicht polizeilich gesuchter Fahrzeugführer würden sofort gelöscht. Bouffier meinte: »Besonders überregional agierenden Straftätern wird deutlich, dass sie in Hessen jederzeit und in allen Teilen des Landes mit der Polizei rechnen müssen«.

Von Datenschützern wurde die Befürchtung geäußert, dass derartige Systeme nach ihrer breiten Einführung auch für die Gewinnung weiterer Daten genutzt werden, z.B. für Bewegungsbilder von angeblichen Terrorverdächtigen oder Drogenkurieren. Der Grünen-Abgeordnete Jürgen Frömmrich beklagte, das Netz elektronischer Überwachung werde immer enger. In Hessen wird nach etwa 40.000 Kennzeichen gefahndet, bundesweit sind es rund 500.000 und in allen Schengen-Staaten etwa 2 Millionen (www.hr-online.de 25.01.2007).

Hessen

Polizeiliche Einsatzprotokolle im Internet

13 Seiten mit 41 Einsatzprotokollen des Polizeipräsidiums Südhessen mit Namen und Daten von 46 kontrollierten BürgerInnen sind versehentlich im Internet gelandet. Ein Kölner Rechtsanwalt entdeckte die Panne bei Online-Recherchen. Das PDF-Dokument war zuvor 11 Monate von der Polizei unbemerkt im Netz gestanden. Die Berichte listeten nicht nur Namen, Geburtsdatum und aktuelle Adresse der Kontrollierten auf, sondern u.U. auch Kfz-Kennzeichen, Automarken, Vorstrafen und Gesetzesverstöße. Es scheine, dass ein Beamter versehentlich den falschen Knopf gedrückt habe, meinte man im Innenministerium. Die Polizei nahm die Daten nach Bekanntwerden sofort aus dem Netz. Da zwischenzeitlich das PDF-Dokument im Cache von Google gelandet war, dauerte es aber eine Woche, bis die Datei hierüber nicht mehr verfügbar war. Die Kontaktaufnahme zu der Firma war nach Polizeiangaben schwierig. Innenminister Volker Bouffier (CDU) sprach von einem bedauerlichen Versehen.

Oppositionsabgeordnete fragten, ob die Entscheidung über die Einstellung von Dokumenten nicht ähnlicher Sicherungen wie beim Internetbanking bedürfe. Der Hessische Datenschutzbeauftragte Prof. Michael Ronellenfitsch forderte organisatorische Vorkehrungen, dass sich so etwas nicht wiederholt, aber auch das Überdenken des technischen Konzepts, wie Daten für das Internet zur Verfügung gestellt werden. Der parteilose Staatssekretär Harald Lemke lehnte die von der Opposition geforderten Erschwernisse ab, weil sie den Erfordernissen polizeilicher Öffentlichkeitsarbeit widersprächen. Pannen ließen sich mit letzter Gewissheit nicht ausschließen.

Als Konsequenz aus der Panne hat die hessische Polizei ihr Online-Publizierungsverfahren geändert. Zugleich warnte das Präsidium eindringlich vor einer Speicherung, Verbreitung und sonstigen Nutzung der Daten, da es sich beim Verbreiten dieser Daten um Verstöße handele, die als Ordnungswidrigkeit oder Straftat geahndet werden könnten. Nicht bekannt wurde, ob gegen die für die Einstellung ins Netz verantwortlichen Polizeibeamte entsprechende Verfahren eingeleitet worden sind.

Das Polizeipräsidium hat sich laut Presseberichten mit den Betroffenen in Verbindung gesetzt und sich ausdrücklich entschuldigt (SZ 17.01.2007, 10; www.spiegel.de 15.01.2007, www.heise.de 16.01.2007; 24.01.2007, 25.01.2007; DSB 2/2007, 4).

Nordrhein-Westfalen

Ärztliche Früherkennungspflicht bis zum 6. Lebensjahr

Die Landesregierung von Nordrhein-Westfalen hat am 30.01.2007 beschlossen, dass für alle Kinder bis zum 6. Lebensjahr ärztliche Früherkennungsuntersuchungen gesetzlich verpflichtend sein sollen. Außerdem werden die Kinderärzte einer »positiven Meldepflicht« unterworfen. Diese soll über einen Datenaustausch zwischen Ärzten, Jugendämtern und Gesundheitsbehörden sichergestellt werden. Wenn sich die Eltern der Untersuchungspflicht für ihre Kinder entziehen, müssen sie mit rechtlichen Sanktionen rechnen. Dies sieht ein vom Düsseldorfer Kabinett beschlossenes »Handlungskonzept für einen besseren und wirksameren Kinderschutz« vor.

Zweck ist nach den Angaben von Familienminister Armin Laschet, dass Gefährdungen des Kindeswohls durch Vernachlässigung oder Misshandlung »früher erkannt werden« können. Dazu gehöre womöglich auch, dass Kinder in kürzeren Abständen untersucht werden. Einbezogen werden auch die Kindergärten, die nach einer geplanten Novelle des Kindertagesstättengesetzes die gesundheitliche Entwicklung der Kinder intensiver beobachten sollen. Die Eltern sollen verpflichtet werden, in den Kitas das sog. Vorsorgeheft ihrer Kinder und entsprechende ärztliche Bescheinigungen vorzulegen. Die in 30 NRW-Städten bestehenden »sozialen Frühwarnsysteme« sollen landesweit ausgebaut werden. Zudem will die Landesregierung ein »Elternbegleitbuch« für Neugeborene entwickeln (vgl. S. 24; SZ 31.01.2007, 5).

Nordrhein-Westfalen

Verfassungsschutz-Trojaner erlaubt

Während über die Erlaubnis der heimlichen Online-Durchsuchung bei Strafverfolgungsbehörden mächtig gestritten wird (S. 21ff., 38), scheint diese Maßnahme für Geheimdienste schon seit Längerem Praxis zu sein. Hierfür gab es – ebenso wie für die Strafverfolgung – bisher keine gesetzliche Erlaubnis. Am 20.12.2006 verabschiedete dann der Düsseldorfer Landtag mit den Stimmen

DATENSCHUTZ NACHRICHTEN

REGISTER FÜR DEN JAHRGANG 2006

Bearbeitung: Karin Bauer

Inhalt

I. Themenübersicht der einzelnen Ausgaben
II. Aufsätze
III. Stellungnahmen, Aufrufe, Presseerklärungen
IV. Rechtsprechung
V. Buch- und Broschürenbesprechung
VI. Deutsche Datenschutznachrichten
VII. Ausländische Datenschutznachrichten
VIII. Welt der Technik
IX. Welt der Gentechnik
X. Stichworte

I. Themenübersicht der einzelnen Ausgaben

1/2006 Datenschutz in Europa
2/2006 Vorratsdatenspeicherung
3/2006 Betrieblicher Datenschutz
4/2006 Big Brother Awards 2006

II. Aufsätze

Alvaro, Alexander	Die Richtlinie zur Vorratsdatenspeicherung **2**, 52ff;
Breyer, Patrick	Vorratsdatenspeicherung - Die totale Protokollierung der Telekommunikation kommt **1**, 17ff;
Dix, Alexander	Zur Prüfpraxis der Aufsichtsbehörden **3**, 122f;
Hülsmann/Schuler	Zur Qualifizierung betrieblicher Datenschutzbeauftragter - Ein Plädoyer für Inhalt statt Form **3**, 108 ff;
Hülsmann, Werner	Gesetzentwurf der Bundesregierung zum Abbau des Datenschutzes **2**, 74ff;
Hustinx, J. Peter	The European Data Protection Supervisor after two years **1**, 4ff;
Lehnert, Matthias	Klage gegen Videoüberwachung an der Universität Münster eingereicht **2**, 78f;
Neundorf, Lutz	Vertrauensvolle Zusammenarbeit zwischen Beauftragten für den Datenschutz und Arbeitnehmervertretungen **3**, 118ff;
Padeluun	Neues Produkt: Privacy-Dongle **2**; 79f;
Puschke, Jens	Die Vorratsdatenspeicherung als Instrument der Strafverfolgung, **2**, 65ff;
Rauhofer, Judith	Die Vorratsdatenspeicherung als Instrument sozialer Kontrolle - eine deutsch-britische Perspektive **2**, 56ff;
Schaar, Peter	Die Kooperation der Datenschutzaufsichtsbehörden am Beispiel der Artikel 29-Gruppe **1**, 7ff;
Schuler, Karin	Europäische Datenschutzorganisationen **1**, 10f;
Schuler, Karin	Mailserver im Konzernverbund: Wer garantiert das Fernmeldegeheimnis **3**, 124ff;
Spaeing, Thomas	Qualitätssicherung im Datenschutz - Das Berufsbild des Datenschutzbeauftragten **3**, 111f;
Weichert, Thilo	Wo liegt Prüm? Der polizeiliche Datenaustausch in der EU bekommt eine neue Dimension **1**, 12ff;
Weichert, Thilo	Volkszählung 2010: Statistische Notwendigkeit oder gläserner Bürger? **1**, 21;
Weichert, Thilo	Vorratsdatenerhebung durch Kfz-Kennzeichen-Scanning - am Beispiel der in Schleswig-Holstein geplanten Regelung **2**, 61ff;
Weichert, Thilo	Datenschutzmanagement **3**, 113ff;
Weichert, Thilo	US-Behördern überwachen die weltweiten Banktransaktionsdaten von SWIFT **3**, 127ff;

III. Stellungnahmen, Aufrufe, Presseerklärungen

ARBEITSKREIS Vorratsdatenspeicherung	
	Aufschub der Protokollierung von Telefon, Handy und Internet gefordert **3**, 150;
	Verfassungsbeschwerde gegen Telekommunikationsgesetz zum Teil ohne Erfolg **3**, 150f;
	Protokollierung der Telekommunikation unter Beschuss **3**, 151;
	Brüssel bestätigt: USA erhalten Zugriff auf vorratsgespeicherte Kommunikationsdaten **4**, 195f;
	Kampagne: Offene Briefe gegen Totalprotokollierung der Telekommunikation **4**, 196;
	»Freiheit statt Angst« **4**, 196f;
	Ministerin Zypries treibt verfassungswidrige Vorratsdatenspeicherung voran **4**, 197;
	Appell an Bundeskanzlerin: Stopp der Vorratsdatenspeicherung gefordert **4**, 198;
Datenschützer, Journalisten, Verbraucherzentralen	
	Widerstand gegen geplante Vollprotokollierung der Telekommunikation **1**, 44f;
Deutsche Bürgerrechtsorganisationen	
	Amerikanischer Abhörskandal erfordert Umdenken auch in Europa **2**, 102;
DVD	Kein betrieblicher Datenschutzbeauftragter für Kleinbetriebe? **1**, 22ff;
FoeBuD	FoedBuD verkauft Schutzhülle gegen unbefugtes Auslesen von RFID-Ausweisen **1**, 46;
	»Befreite Dokumente« für alle im Internet abrufbar **1,** 46;
	FoeBuD entwickelt »PrivacyDongle« gegen Vorratsdatenspeicherung **4**, 199;
FoeBuD, DVD	Schnüffelchips: RFID-Industrie setzt auf PR-Offensive statt auf konstruktiven Dialog **1**, 45f;
	Thema verfehlt: Das Positionspapier des Handels zum RFID-Einsatz **3**, 149;
Internationale Liga für Menschenrechte	
	»Internationale Liga für Menschenrechte« protestiert gegen geheimdienstliche Überwachung ihres Präsidenten **1**, 47;
Internationale Liga für Menschenrechte/FoeBuD	
	Entscheidung des Europäischen Gerichtshofs gegen Fluggastdatentransfer an US-Sicherheitsbehörden **2**, 103;
Komitee für Grundrechte und Demokratie	
	Nein zur elektronischen Gesundheitsdatei **4**, 199;

IV. Rechtsprechung

EUGH	EU für Passenger-Name-Record-Regelung unzuständig **3**, 116;
BGH	Keine schriftliche Dokumentationspflicht bei Anlageberatung **1**, 40;
	Nur 10 Jahre Ansprüche aus Namensschutz für Erben **4**, 191;
	T-Online darf Internet-Verbindungsdaten nicht speichern **4**, 191f;
	Schadensersatz für Verletzungen des Rechts am eigenen Bild **4**, 192;
	Sammelklagebefugnis von Verbraucherverbänden für Kunden **4**, 192;
BVerfG	Für die Zukunft: Präventiver Persönlichkeitsschutz geht vor Äußerungsfreiheit **1**, 40;
	Fahnder dürfen Handy-Verbindungsdaten einsehen **2**, 96;
	Eingebürgerte Türken müssen Auskunft geben über Repatriierung **2**, 96;
	Rasterfahndung 2001/2002 verfassungswidrig **2**, 97;
	Vager Verdacht genügt nicht für Durchsuchung **3**, 146;
	Richterbeschlüsse nur mit konkreter Benennung der Straftat **3**, 146f;
	Selbstöffnung hindert Unterlassungsansprüche gegen Foto-Veröffentlichung **4**, 190;
	IMSI-Catcher-Regelung verfassungsgemäß **4**, 190f;
BAG	Lohnfortzahlung nur nach Schweigepflichtentbindung **1**, 41;
BayVerfGH	Durchsuchungen bei Schleierfahndung eingegrenzt **1**, 40f;
OVG Rheinland-Pfalz	Polizeischutz-Überwachung für Nachbarn verhältnismäßig **1**, 41;
Hessischer VGH	Akteneinsicht für Flughafen-Ausbaugegner **1**, 41;
LAG Köln	Videoüberwachung bei verdächtigem Mitarbeiter zulässig **3**, 147;
LG Darmstadt	Verbindungsdatenspeicherung nur für Rechnungszwecke **1**, 42;

LG Flensburg	Keine Strafanzeigen-Maschinerie wegen Urheberrechtsverletzungen **1**, 42;
LG Hamburg	Schadensersatz für Verletzungen am eigenen Bild **4**, 192;
	Schutz vor kalten Marktforschungs-Werbeanrufen **4**, 192;
LG Potsdam	Cicero-Redaktionsdurchsuchung rechtmäßig **2**, 97;
LSG Darmstadt	Vorlage von Kontoauszügen bei Sozialleistungsbezug nicht erforderlich **3**, 147;

V. Buch- und Broschürenbesprechung

Bergmann, Lutz/Möhrle, Roland	Datenschutzrecht **4**, 193;
Bohnstedt, Jan	Fernwartung - Die rechtlichen Grenzen des IT-Outsourcing durch Banken **3**, 147f;
Ehmann, Eugen (Hrsg.)	Datenschutz kompakt **4**, 193f;
Gola, Peter	Datenschutz und Multimedia am Arbeitsplatz **1**, 43;
Gola, Peter/Jasper, Andreas	Das BDSG im Überblick **1**,43;
Gola, Peter/Schomerus, Rudolf	BDSG - Bundesdatenschutz - Kommentar **4**, 194;
Scheja, Gregor	Datenschutzrechtliche Zulässigkeit einer weltweiten Kundendatenbank **2**, 98;
Siemen, Birte	Datenschutz als europäisches Grundrecht **2**, 98f;
Simitis, Spiros (Hrsg.)	Bundesdatenschutzgesetz **3**, 148;
Singelnstein, Tobias/Stolle Peer	Die Sicherheitsgesellschaft **2**, 100;
Stylianidis, Annette	Rechtsfolgen privater Vaterschaftsbegutachtung **2**, 100f;
Talidou, Zoi	Regulierte Selbstregulierung im Bereich des Datenschutzes **2**, 99f;

VI. Deutsche Datenschutznachrichten

Baden-Württemberg

Gesinnungstest bei Einbürgerung von Muslimen **1**, 30f;
GVU-Fahnder betätigen sich als Raubkopierer **2**, 85;
Casino-Einlasskontrolle durch Video-Gesichts-Mustererkennung **2**, 85;

Bayern

Versteckte Kamera in Münchner Bordell **1**, 31;
PAG mit vielen informationellen Befugnissen **1** 31f;
Streit vor Gericht über Verfassungsschutzbeobachtung **3**, 136;
Gentechnikgegner vom Staatsschutz überwacht **4**, 173;
Neue Sexualstraftäterdatei **4**, 173,

Berlin

Terrorverdachtsliste stoppt Gründstückskauf **2**, 85f;
Museumswachleute videoüberwachten unbemerkt Merkels Wohnzimmer **2**, 86;
Verkehrsüberwachung mit Weltraumtechnik **3**, 136;
Verfassungsschutz beobachtet Regierungskritiker **3**, 136f;

Brandenburg

Kabinett will dauerhafte Videoüberwachung **1**, 32;
Jauch gegen »Bild am Sonntag« wegen Verleumdung **4**, 173;
Email-Überwachung in der CDU-Geschäftsstelle **4**, 173f;

Bremen

Datei für Stalker **1**, 32;

Bund

PKG neu besetzt **1**, 25;
Kommt doch noch der Geheimdienstbeauftragte? **1**, 25f:
Birthler weitere fünf Jahre Stasiakten-Beauftragte **1**, 26;
Mobile Biometrie-Identifikation **1**, 26;
CDU-CSU-Landespolitiker fordern Fußfessel für Ausländer **1**, 26f;
Fotos im Ausländerzentralregister u.v.m. **1**, 27;
Behördliche Vaterschaftsanfechtung bei »Scheinvätern« **1,** 27;
Praxis des Kontoevidenzverfahrens mangelhaft **1**, 27f;
Mit Kuno gegen EC-Kartenbetrug **1**, 28;
Rechnungshof fordert Sozialdatenabgleich **1**, 28;
Gesundheits-Pflichtuntersuchung bei Kleinkindern geplant **1**, 28;
BKA nutzt Easy **1**, 28;
Abgeordneten-Nebeneinkünfte werden öffentlich **1**, 28f;
Unternehmensdaten werden über Internet verfügbar **1**, 29;
Kommt die PKW-Maut doch? **1**, 29;
Schäuble: Maut-Daten zur Strafverfolgung nutzen **1**, 29f;
Telekommunikationsüberwachung wieder stark gestiegen **2**, 81;
Terrorismusgesetze: Zugriff auf Konto- und Kfz-Daten für Geheimdienste **2**, 81f;
Justizministerium bereitet Wiedereinführung von Kronzeugenregelung vor **2**, 82;
Immer mehr Eintragungen beim Kraftfahrtbund **2**, 82;
Verfassungsschutz überwacht Abgeordnete **2**, 82f;
Grüne wollen Meldepflicht für Ausländer abschaffen **2**, 83;
BND bespitzelte Journalisten im großen Stil **2**, 83f;
Einheitliche Standards für Einbürgerung **2**, 84;
Terrorismusbekämpfungs-Ergänzungsgesetz **3**, 131f;
Bundesrat gegen Veröffentlichung von Agrarsubventionsempfängern **3**, 132;
Einigung über zentrale Anti-Terror-Datei **3**, 132f;
Abhöraktion und dubiose Ermittlungen gegen Entführungsopfer el-Masri **3**, 133f;
Grüne fordern Informationspflicht für Unternehmen bei Datenschutzverstößen **3**, 134;
Schufa gewährt Betroffeneneinblick per Internet **3**, 134;
NS-Archiv in Bad Arolsen wird für Forschende geöffnet **3**, 134;
Auch Jugendliche spitzelten für die Stasi **3**, 134;
Verfassungsschutz beobachtet Abgeordnete als Extremisten **3**, 134f;
TK-Überwachungen steigen weiter **4**, 167;
2005 nur noch sieben Große Lauschangriffe **4**, 167;

Internet-Überwachung verstärkt **4**, 167;
Computerstrafrecht wird verschärft **4**, 167f;
Ausländer-Ausweis geplant **4**, 168;
Sicherheitsbehörden haben Zugriff auf 197 Dateien **4**, 168f;
Sexualtäter-Internetpranger jetzt auch in Deutschland? **4**, 169;
Schily wird Aufsichtsrat in Biometrie-Unternehmen **4**, 169f;
Telemediengesetz: Kundendaten zur Strafverfolgung? **4**, 170;
Darlehensverkauf verletzt Bankgeheimnis **4**, 170f;
Finanzämter prüfen Banken-Jahresbescheinigungen **4**, 171;
Schufa löscht Bagatellfälle früher und ändert Scoring **4** 171;
»Lesereporter« der Bildzeitung auf Bilderjagd **4**, 171;
Netzagentur geht gegen Telefon-Abzocker vor **4**, 171;
Regierung beschließt registergestützte Volkszählung **4**, 171f;
Geplante SchülerInnen-Datenbank stößt auf Ablehnung **4**, 172f;

Hamburg

Bezahlen mit Fingerabdruck im »Night Fever« **2**, 86;
Senat will bei Islamisten lückenlosen Datenaustausch **2**, 86f;
Mehr Gewalt trotz Videokameras **3**, 137;

Hessen

Massengentest soll Kindervergewaltiger ermitteln **1**, 32;
Jung soll illegal vertrauliche Personalinformationen entgegen genommen haben **2**, 87;
Polizei möchte auf LKW-Maut-Daten zugreifen **3**, 137;
Ausweitung der Videoüberwachung **4**, 174f;

Mecklenburg-Vorpommern

Polizeirechtsverschärfung auch im Nordosten **2**, 87;

Mehrere Länder

Sparkassen testen elektronische Signatur **1**, 30;
Zuviel Videoüberwachung an Hochschulen **2**, 84f;

Niedersachsen

Polizei kontrolliert Journalisten-Telefone **1**,32f;
Anonyme Internet-Anzeigen bringen nichts außer Ärger **2**, 87;
Neue Datenschutzorganisation des Landes umstritten **2**, 87f;
Nach Föderalismusreform kein Datenschutz mehr für Gefangene? **3**, 137;

Nordrhein-Westfalen

Neues Polizei-Auskunftssystem Polas **1**, 33;
Verkehrsüberwachung mit Weltraumtechnik **3**, 136;
Opposition kritisiert geplante Verfassungsschutzgesetz-Novellierung **3**, 137f;
Handydatenabgleich führt zu Einbrecherbande **4**, 175;

Rheinland-Pfalz

Gesichtserkennungstest am Mainzer Hauptbahnhof **3**, 138;

Saarland

Datenschützer gegen neues Polizeigesetz **2**, 88;
Informationsfreiheitsgesetz beschlossen **3**, 138;

Sachsen

Bisher größter Massen-Gentest **3**, 138f;
Verfassungsschutz beobachtet illegal Organisierte Kriminalität **4**, 175;

VII. Ausländische Datenschutznachrichten

Bulgarien

Regierung tut sich mit der Aktenveröffentlichung schwer **3**, 142;

China

Korrupte Geschäftsleute am Pranger **1**, 37;
Militär-Hacker greifen USA an **1**, 37;
Umfassende Internet-Kontrolle **1**, 37f;
Identifizierung aller Handy-Nutzer **1**, 38;
Schule verlangt Finderabdrücke **1**, 38;

EU

Strafregister-Netz im Echtbetrieb **3**, 139;
EU soll fremde Geheimdienste zentral kontrollieren **3**, 139;
CIA erhält künftig Flugpassagierdaten **4**, 176;

Frankreich

Anti-Terror-Gesetz verabschiedet **1**, 34;
Motorrad-Polizisten mit versteckter Kamera **1**, 34;
Metalldetektoren und Kameras an Schulen **1**, 34;
Elektronische Fessel für Serientäter **1**, 34;

Griechenland

Abhörskandal bis in die politischen Spitzen von Athen **2**, 89f;

Großbritannien

Neuer Einwanderungstest prüft »Britishness« **1**, 33;
Schadenersatz wegen Spam **1**, 33;
Kinder dürfen für Passfotos lächeln **1**, 33;
Staatliche Videoüberwachung für jedermann **1**, 33f;
Spezialbehörde SOCA soll Schwerverbrecher jagen **2**, 88;
Britischer Personalausweis bleibt freiwillig **2**, 88f;
Scotland-Yard-Chef wegen Telefonüberwachung in Bedrängnis **2**, 89;
Innenministerium will Schlüsselherausgabe erzwingen **3**, 139f;
Satellitenüberwachung von Sexualstraftätern angeregt **3**, 140;
Ausweitung der Verkehrs-Maut geplant **3**, 140;
Datenschützer fordern Umdenken bei der Überwachung **4**, 177f;
Allgegenwärtige Videoüberwachung **4**, 178;
»Eingreifende Videoüberwachung« **4**, 178;
Journalist soll Prinz Charles abgehört haben **4**, 178f;
Mülltonnen werden verwanzt **4**, 179;
Terror-Verdächtigenliste im Internet **4**, 179;
Handflächen-Scanning in der Schule **4**, 179;
Bier gegen Fingerabdrücke **4**, 179f,

Hongkong

Parlament beschließt Überwachungsgesetz **4**, 185f;

Irland

Bürgerrechtler gegen TK-Vorratsdatenspeicherung **3**, 140f;

Italien

Laziogatte belastet Rechtsregierung kurz vor der Wahl **2**, 89;
Abhören im Land der Tifosi und der Pasta **4**, 180ff;
Zentrale Steuerdatei wurde umfangreich ausspioniert **4**, 183;

Japan

Bankkundenidentifikation mit Venenmuster **2**, 92;

Kolumbien

Biometrischer Personalausweis mit Zentral-Datei **2**, 92;

Niederlande

Oppositionsüberwachung durch Nachrichtendienst AIVD **1**, 34f;

Österreich

Hohe Hürden hindern Einbürgerung **1**, 35;
Anonyme Nummernbriefkästen verschwinden **3**, 141;
SWIFT bei österreichischem BigBrotherAward Doppelsieger **4**, 176f;

Polen

Priesterbespitzelung **3**, 141;

Schweden

Mit Tricks gegen die City-Maut **3**; 141;

Schweiz

Bankgeheimnis weiterhin ohne Verfassungsrang **2**, 90;
Umfassende Internetüberwachung und zentrale Biometriedatei geplant **3**, 142;
Anti-Terror-Pakete stoßen auf Widerstand **4**, 183f;

Ungarn

Computerspionage für Wahlkampfzwecke **2**, 90;
RFID-Test mit Flughafenbesuchern **4**, 184;

USA

Patriot Act bleibt kurzfristig weiter bestehen **1**, 35;
Auslandsgeheimdienst hat Amerikaner ausspioniert **1**, 35f;
American Civil Liberties Union **1**, 36;
Schärfere Paparazzi-Regelungen in Kalifornien **1**, 36;
Sexualstraftäter auf der Plakatwand **1**, 37;
Verteidigungsministerium muss Guantanamo-Häftlingsnamen nennen **2**, 90;
Mehr als 200.000 Personen auf Terroristen-Liste **2**, 91;
Patriot Act wurde weitgehend unbefristet verlängert **2**, 91;
CIA-Agenten-Dekonspiration per Internet **2**, 91;
Kreditkartendaten von Zeitungskunden auf Packpapier **2**, 91;
TK-Vorratsdatenspeicherung in USA illegale Praxis **2**, 91f;
Drohnen im Polizeieinsatz **3**, 142f;
AT&T ändert Privacy-Policy **3**, 143;
Geheimdienste werten sog. Web2.0-Angebote systematisch aus **3**, 143f;
Wirtschaftsspionagebekämpfung durch Telefonüberwachung **4**, 184;
Richterin stoppt Bushs Lauschprogramm **4**, 184;
Kreditkarte funkt per RFID Inhaberdaten, **4**, 184f;
CIA erhält künftig Flugpassagierdaten **4**, 176;
Schwarzenegger gegen kalifornisches RFID-Gesetz **4**, 185;
Riesige Anti-Terror-Datei **4**, 185;

VIII. Welt der Technik

Mit Laser durch Wände blicken **1**, 38;
Schweiß soll Biometrie sicherer machen **1**, 38;
iTunes spioniert Nutzerverhalten aus **1**, 38f;
Hilferuf per Handy **1**, 39;
Sinnvolle RFID-Anwendungen im Strafvollzug **1** 39;
Digitale Erpressung mit Schadprogrammen **2**, 93;
Wie funktioniert forensische Phonetik? **2**, 93;
Viren gefährden RFID-Funkchip **2**, 93;
Ungeschützte Webcam-Bilder im Internet **2**, 93;
Lügendetektion per Mimikauswertung **2**, 93f;
Kameras hinterlassen »Fingerabdruck« **2**, 94;
Substanzanalysen beim Fingerabdruck ermöglichen weitgehende Rückschlüsse **2**, 94;
Handyortung wird zur Massendienstleistung **3**, 144;
Firefox dank Datenschutz auf dem Vormarsch **3**, 144f;
Mit Giropay im Internet bezahlen **3**, 145;
Phishing jetzt auch über Telefon **3**, 145;
CCC: Wahlcomputer unsicher **4**, 186;
Gesichtersuche im Internet **4**, 186;
Durchstrahlung zwecks Terrorabwehr **4**, 186f;
IBM bietet Reisenden-Kontrollsystem an **4**, 187;
Chipkarte erzeugt Einmalpasswort **4**, 187;
Babyschrei-Monitor ermittelt Ursachen **4**, 187;
Patientenidentifikation mit RFID **4**, 187;
Mini-Funkchips mit Riesenspeicher **4**, 187f;
IBM will »intelligente Videoüberwachung« **4**, 188;
Nachtsichtgerät für Autofahrer **4**, 188;

IX. Welt der Gentechnik

Gentest klärte erstmals Schuld von Hingerichtetem (USA) **1**, 39;
DNA-Analyse immer schneller und billiger **2**, 94f;
Familienermittlungen über genetische Fingerabdrücke **2**, 95;
Menschliches Erbgut jetzt vollständig bekannt **3**, 145;
UK-Biobank mit 500.000 Proben geplant **4**, 188f;

X. Stichworte

A

Abgeordnete **1**, 28f; **2**, 83; **3**, 135f; **4**, 157f;
Abhören **1**, 21; **2**, 89; **3**, 133f; **4**, 180;
Äußerungsfreiheit **1**, 40;
Agrarsubvention **3**, 132;
AIVD **1**, 34;
Akteneinsicht **1**, 41;
ALCEI **1**, 11;
American Civil Liberties Union (ACLU) **1**, 36;
Amerikanischer Datenschutz **1**, 36;
Anlageberatung **1**, 40;
Anti-Terror **1**, 34, 35, 36; **3**, 132f; **4**, 183, 185;
Anti-Terror-Datei **3**, 132f; **4**, 158;
Arbeitnehmer **1,** 41;
Arbeitnehmervertretung **3**, 118f;
Arge Daten **1**, 11;
Artikel 29 - Gruppe **1**, 7;
Association Electronique Libre (AEL) **1**, 10;
AT&T **3**, 143;
Aufsichtsbehörden **1**, 23; **2**, 87f; **3**, 122f;
Auftragsdatenverarbeitung **3**, 125;
Ausbildung betrieblicher Datenschutzbeauftragter **3**, 109;
Ausländer **1**, 27; **2**, 83; **4**, 168;
Ausländerausweis **4**, 168;
Ausländerzentralregister **1**, 26;
Auto **4**, 188;

B

Babyschreimonitor **4**, 187;
Bad Arolsen **3**, 134;

Bagatellfälle **4**, 171;
Bandinformationen **1**, 38f;
Banken **1**, 27, 40; **2**, 81, 90, 92; **3**, 127f, 147; **4**, 170, 171;
Bankgeheimnis **2**, 90;
Befreite Dokumente **1**, 46;
Berufsbild betrieblicher Datenschutzbeauftragter **3**, 111;
Berufsgeheimnis **2**, 74;
Betrieblicher Datenschutz **1**, 22; **3**, 107, 108ff, 115, 125;
Betrieblicher Datenschutzbeauftragter **1**, 22ff; **2**, 75ff; **3**, 108ff;
Bewegungsprofil **2**, 62;
Bier **4**, 179;
BigBrotherAwards **4**, 156ff;
Bildzeitung **4**, 171;
Biobanken **4**, 188;
Biometrie **1**, 26, 38; **2**, 92; **3**, 142; **4**, 169;
Birthler-Behörde **1**, 26;
Bits of Freedom **1**, 11;
Bordell **1**, 31;
Briefkästen **3**, 141;
Britishness **1**, 33;
Bürgerrechte **1**, 10; **2**, 54f, 102;
Bürokratieabbau **1**, 74;
Bundesdatenschutzgesetz (BDSG) **1**, 22f; **2**, 54, 74ff; **3**, 108, 125, 130, 134;
Bundeskanzlerin **2**, 86; **4**, 198;
Bundeskriminalamt (BKA) **1**, 28;
Bundesnachrichtendienst **1**, 25; **2**, 83f; **3**, 131f;
Bundesnetzagentur **4**, 171;
Bundesverteidigungsminister **2**, 87;

C
Casino **2**, 85;
CD-Brenner **4**, 162;
CDU-Geschäftsstelle **4**, 173;
Chipkarte **4**, 187;
CIA **2**, 91; **4**, 176;
Cicero-Redaktion **2**, 97f;
Cold Calls **3**, 130;
Computerspionage **2**, 90;
Computerstrafrecht **4**, 167;

D
Darlehensverkauf **4**, 170;
Datenschutzaufsichtsbehörden **1**, 7, 10; **2**, 74ff, 87f; **3**, 119, 112, 129; **4**, 177f;
Datenschutzmanagement **3**, 113ff;
Datenschutzrichtlinie **1**, 4;
Datenschutzverstoß **3**, 134;
Demonstration **1**, 13; **3**, 152; **4**, 196;
Digital Rights **1**, 10;
Directive **1**, 4;
DNA **1**, 13; **2**, 94f;
DNA-Analyse **2**, 94;
DNA-Profile **1**, 13;
Doping **3**, 130;
Drohnen **3**, 142;
Durchsuchung **3**, 146; **4**, 191;

E
Easy **1**, 29;
EC-Kartenbetrug **1**, 28;
Einbürgerung **1**, 9, 30, 35; **2**, 84, 96; **3**, 136;;
Einwanderungstest **1**, 33;
Electronic Frontier Finland (EFFI) **1**, 10;
Elektronische Gesundheitskarte (eGK) **4**, 199;
Elektronische Signatur **1**, 30;
El-Masri **3**, 133f;
Email-Überwachung **4**, 173f;
Entbürokratisierung **1**, 24;
Erbgut **3**, 145;
EU-Kommission **1**, 5; **2**, 57f; **3**, 128f, 139;
Europa **1**, 5ff, 12, 41; **2**, 52, 56ff;
Europäischer Datenschutzbeauftragter (EDSB) **1**, 4ff;
Europäische Datenschutzorganisationen **1**, 10f;
European Data Protection Supervisor **1**, 4f;
European Digital Rights (EDRI) **1**, 10;

F
Falschverdächtigung **1**, 19;
Familienermittlung **2**, 95f;
Fernmeldegeheimnis **3**, 124;
Finanzamt **4**, 171;
Fingerabdruck **1**, 13, 38; **2**, 86, 94, 95; **4**, 179f;
Firefox **3**, 144f;
Fischer, Joschka **1**, 20;
Flüchtliungspolitik **1**, 16;
Fluggastdaten **2**, 103; **4**, 176;
Flughafen **4**, 184;
Föderalismus **3**, 137;
Forensische Phonetik **2**, 93;
Foto-Veröffentlichung **4**, 190;
Fußfessel **1**, 26, 34;
Funkchip **4**, 187;

G
Gefährder-Datei **1**, 32;
Gefangene **3**, 137;
Geheimdienstbeauftragter **1**, 25;
Geheimdienste **1**, 25; **3**, 139, 143f;
Geheimdienstkontrolle **3**, 139;
Geldkontrolle **3**, 129;
Gentest **1**, 39; **4**, 173;
Gesamtverband der Deutschen Versicherungswirtschaft (GDV) **4**, 163;
Gesichtserkennung **3**, 138; **4**, 186;
Gesinnungstest **1**, 9, 30;
Gesundheit **1**, 28; **4**, 199;
Giropay **3**, 145;
Gössner, Rolf **1**, 47;
Google **2**, 79;
Großer Lauschangriff **4**, 167;
Grundrechte **2**, 60, 67;
Guantanamo **2**, 90f;

H
Hacker **1**, 37;
Handelsregister **1**, 29;
Handflächenscaning **4**, 179;
Handy **1**, 38, 39; **2**, 96; **3**, 144; **4**, 175;
Handy-Ortung **3**, 144;
Handy-Verbindungsdaten **2**, 96;
Hochschulen **2**, 84f;
Holocaust-Archiv **3**, 134;
Homosexualität **1**, 31;
Humangenom **3**, 145;

I
Identifizierungspflicht **3**, 150;
Identitätsdiebstahl **3**, 134;

Imaginons un Réseau Internet Solidaire (IRIS) **1**, 10;
IMSI-Catcher **4**, 190f;
Informationsfreiheitsgesetz (IFG) **1**, 46; **3**, 138;
Innenminister **1**, 15, 27, 28, 29; **3**, 135, 139; **4**, 158f;
Innere Sicherheit **1**, 15;
Internationale Zusammenarbeit **1**, 8;
Internationaler Suchdienst **3**, 134;
Internet **1**, 29, 33, 37; **2**, 87, 91, 93; **3**, 143; **4**, 186;
Internet-Kontrolle **1**, 37; **4**, 167;
IT-Outsourcing **3**, 147;
iTunes **1**, 38f;

J
Jauch, Günter **4**, 173;
Journalisten **1**, 32f; **2**, 83f;
Jugendliche **3**, 134;
Jung, Franz-Josef **2**, 87;

K
Kameras **2**, 94;
Karlsruher Erklärung **1**, 15;
Kinder **1**, 28, 33;
Kfz **1**, 13, 29; **2,** 81;
Kfz-Kennzeichen-Scanning **2**, 60ff,
Kleinbetrieb **1**, 32;
Kleinkinder-Pflichtuntersuchung **1**, 28;
Kommunikationsdaten **2**, 58f;
Kontoevidenzverfahren **1**, 27;
Konzern-Outsourcing **3**, 124;
Korruption **1**, 37;
Kraftfahrtbundesamt (KBA) **2**, 82;
Kreditkarten **2**, 91;
Kronzeugenregelung **2**, 82;
Kulturministerkonferenz **4**, 161;
Kundendaten **4**, 170;
Kundendatenbank **2**, 98;
Kuno **1**, 28;

L
Laser **1**, 38;
Lauschangriff **4**, 167, 184;
Laziogate **2**, 89;
Leserreporter **4**, 171;
Liberty **1**, 10f;
Lichtbilder **1**, 27, 33;
LKW-Maut-Daten (siehe auch Maut) **3**, 137;
Lohnfortzahlung **1**, 41;
Lügendetektion **2**, 93;

M
Mailserver **3**, 124f;
Mannvernd **1**, 11;
Marktforschungs-Werbeanrufe **4**, 192;
Massengentest **1**, 32; **3**, 138;
Massenprotokollierung **1**, 19;
Maut **1**, 29; **3**, 137, 140; **4**, 189;
Menschenrechte **2**, 51, 86;
Merkel, Angela **2**, 86
Metalldetektoren **1**, 34;
Migrationspolitik **1**, 16;
Militär Hacker **1**, 37;
Milli Görüs **3**, 136;
Mimikauswertung **2**, 93;
Mobile Biometrieidentifikation **1**, 26;
Motorrad-Polizisten **1**, 34;
Mülltonnen **4**, 179;
Muslime **1**, 9, 30;

N
Nachrichtendienste **1**, 34f;
Nachtsichtgerät **4**, 188;
Namensschutz **4**, 191;
National Security Agency (NSA) **1**, 35; **2**, 102;
Nebeneinkünfte **1**, 28;
NS-Archiv **3**, 134;
Nummernbriefkasten **3**, 141;

O
Oettinger, Günter **1**, 21;
Organisierte Kriminalität **1**, 31, 41; **2**, 52ff, 58f, 88; **4**, 175;

P
Paparazzi **I**, 36;
Parlamentarisches Kontrollgremium (PKG) **1**, 25;
Passfoto **1**, 33;
Passenger Name Record (PNR, siehe auch Fluggastdaten) **3**, 146;
Passwort **4**, 187;
Patientenidentifikation **4**, 187;
Patriot Act **1**, 35; **2**, 91;
Personalausweis **2**, 89f, 92;
Persönlichkeitsschutz **1**, 40;
Phonetik **2**, 93;
Pflichtuntersuchungen **1**, 28;
Phishing **3**, 145;
PKW-Maut (siehe auch Maut) **1**, 29;
Polas **1**, 33;
Polizei **1**, 26, 31, 33; **2**, 62, 87;
Polizeiaufgabengesetz **1**, 31f;
Polizeiauskunftssystem **1**, 33;
Polizeirecht 1, 31; **2**, 87, 88; **4**, 157f;
Polizeischutz **1**, 41;
Priesterspitzel **3**, 141;
Prinz Charles **4**, 178f;
Privacy-Dongle **2**, 79f; **4**, 199;
Privacy Enhancing Technologies **3**, 114;
Privacy International **1**, 11;
Privacy Ukraine **1**, 11;
Provider **3**, 125;
Prüm **1**, 12ff;

Q
Qualitätskontrolle (bDSB) **3**, 110, 111f, 114f;

R
Rasterfahndung **2**, 97;
Raubkopien **2**, 85;
Rechnungshof **1**, 28;
Recht am eigenen Bild **4**, 192;
Regimekritiker **3**, 136f;
Reisenden-Kontrollsystem **4**, 187;
Repatriierung **2**, 96f;
RFID **1**, 39, 45f; **2**, 93; **3**, 149; **4**, 184f;
RIPA **2**, 58f;
Röntgen **4**, 186;

S
Satellitenüberwachung **3**, 140;
Schadprogramme **2**, 95;
Scheinehen **1**, 27;

Scheinväter **1**, 27;
Schleierfahndung **1**, 40f;
Schily, Otto **4**, 169;
Schleppnetz-Fahndung **2**, 61;
Schufa **3**, 134; **4**, 171;
Schüler-Datenbank **4**, 172;
Schüler-ID **4**, 161, 172;
Schulen **1**, 34, 38; **4**, 172f, 179;
Schwarzbuch Datenschutz **3**, 126;
Schwarzenegger **4**, 185;
Schweigepflichtentbindung **1**, 41;
Schweiß **1**, 38;
Scoring **4**, 171;
Scotland Yard **2**, 89;
Selbstkontrolle **1**, 23f;
Sexualstraftäter **1**, 34, 37; **3**, 140; **4**, 169, 173;
Sicherheitsbehörden-Dateien **4**, 168;
Signatur **1**, 30;
SOCA **2**, 88;
Sozialdatenabgleich **1**, 28;
Spam **1**, 33;
Sparkassen **1**, 30;
Spielhallen **2**, 85;
Staatsangehörigkeit **1**, 30;
Staatsbürgerschaftsgesetz **1**, 35;
Staatsschutz **4**, 173;
Stalker **1**, 32;
Stasiakten **1**, 26;
Stasi **3**, 134, 142;
Steuerdatei **4**, 183;
Statewatch **1**, 11;
Strafregister-Netz **3**, 139;
Strafverfolgung **1**, 13, 17, 32, 39; **2**, 52ff; 56ff, 62f, 65f, 68ff; **4**, 170;
Strafvollzug **1**, 39; **3**, 137;
Supervision **1**, 5;
Surveillance Society **4**, 177;
SWIFT **3**, 127f; **4**, 156f, 176f;

T
Tasern **1**, 31f;
Telefon-Abzocker **4**, 171;
Telefonmarketing **3**, 130;
Telefon-Phising **3**, 145;
Telefonüberwachung **1**, 32f; **2**, 57, 87, 89, 91f; **3,** 143;
Telekommunikation **1**, 17f, 28; **2**, 66, 81; **3**, 124f, 150; **4**, 167, 196;
Telekommunikationsüberwachung **2**, 81; **4**, 167;
Telemediengesetz (TMG) **4**, 170;
Terrorismus **1**, 8, 13; **2**, 56f, 81f, 86, 86f, 91; **3**, 128f, 131f;
Terrorismusbekämpfungs-Ergänzungsgesetz **3**, 131f;
Terroristenliste **2**, 91;
Terrorverdachtsliste **1**, 85; **4**, 179;
Todesstrafe **1**, 39;
T-Online **4**, 191;
Totalprotokollierung **4**, 196;
Transparenzinitiative **3**, 132;
Türken **2**, 96;

U
Universität **2**, 78f;
Uniwagnis **4**, 163;
Unterhaltungselektronik **4**, 162;
Unternehmensdaten **1**, 29;
Urheberrecht **1**, 42; **2**, 85;

V
Vaterschaftsanerkennung **1**, 27;
Vaterschaftstest **2**, 100;
Verbindungsdaten **1**, 43; **4**, 191 f;
Venenmuster **2**, 92;
Vergewaltiger **1**, 32;
Verfassungsschutz **1**, 47; **2**, 82f; **3**, 134f, 136f, 137; **4**, 175;
Verfassungsschutzgesetz **3**, 137;
Verfügbarkeit **1**, 12;
Verkehrs-Maut (siehe auch Maut) **3**, 140;
Versicherungswirtschaft **4**, 163f;
Videoüberwachung **1**, 24, 32; **2**, 78f, 84f; **3**, 137; **4**, 174f, 178;
Volkszählung 2010 **1**, 21; **2**, 59; **4**, 171;
Vorratsspeicherung **1**, 17f, 44; **2**, 51, 52ff; 56ff, 65f, 79, 91; **3**, 140f, 150; **4**, 195, 197, 198, 199;

W
Wahlcomputer **4**, 186;
Wahlkampf **2**, 90;
Web 2.0 **3**, 149;
Webcam **2**, 93;
Weltraumtechnik **3**, 136;
Wirtschaftskorruption **1**, 37;
Wirtschaftsspionage **4**, 184;
Working Paper **1**, 8;

Z
Zensus **1**, 21;
Zippo-A **2,** 93;
Zuhälter **1**, 31;

Datenschutz Nachrichten – Jahresregister 2006
Herausgegeben von der Deutschen Vereinigung für Datenschutz e.V. – DVD
Geschäftsstelle: Bonner Talweg 33-35, 53113 Bonn, Tel. 0228-222498, E-Mail: dana@datenschutzverein.de
Bearbeiterin: Karin Bauer — Beilage zur DANA 1/2007

von CDU und FDP eine Änderung des Verfassungsschutzgesetzes, die dem Landesamt für Verfassungsschutz (LfV) die Befugnis zum verdeckten Zugriff auf »Festplatten« und andere »informationstechnische Systeme« einräumt. Die seit Januar 2007 in Kraft befindliche Regelung ist nach Ansicht von FDP-Innenminister Ingo Wolf ein »Quantensprung«. Nach Mitteilung von Ministeriumssprecherin Dagmar Pelzer gehe es darum, Computer extremistischer Terroristen heimlich zu kontrollieren, etwa bei der Gefahr von Terroranschlägen, bei Mitgliedschaft in einer terroristischen Vereinigung oder bei Mord. Bisher sei das Gesetz noch nicht angewandt worden. Wolf ist zugleich gegen eine Änderung der Strafprozessordnung mit entsprechenden Befugnissen für Polizei und Staatsanwaltschaft: »Die Beweislast liegt bei Herrn Schäuble. Nach derzeitigem Stand sehen wir keine Notwendigkeit.«

Am 09.02.2007 legte Rechtsanwalt Fredrik Roggan für die Mülheimer Bürgerrechtlerin Bettina Winsemann (»Twister«) und ein Mitglied der Linkspartei Verfassungsbeschwerde ein. Nach Roggans Ansicht verletzt die Regelung nicht nur die Privatsphäre, sondern auch das Grundrecht auf Unverletzlichkeit der Wohnung: »In jedem Fall ist das Gesetz verfassungswidrig, weil es keine Vorkehrungen zum Schutz der Intimsphäre enthält. Wer in Nordrhein-Westfalen auf seinem Rechner auch tagebuchartige Aufzeichnungen oder Fotos von nahen Angehörigen speichert, kann nicht mehr sicher sein, dass solche höchstpersönlichen Sachverhalte nicht staatlicherseits heimlich ausgespäht werden können«. Der niedersächsische Landtag, der sich schon mit dem verfassungswidrigen Vorhaben präventiver Telefonüberwachung hervorgetan hat, bastelt an einer entsprechenden Regelung (Störing c't 5/2007, 60; Financial Times Deutschland 06.02.2007 online; PM HU 09.02.2007; www.heise.de 10.02.2007).

Nordrhein-Westfalen

Obligatorischer Deutschtest für Vierjährige

Als erstes Land führt Nordrhein-Westfalen für alle vierjährigen Kinder einen obligatorischen Deutschtest ein. Familienminister Armin Laschet (CDU) kündigte am 12.02.2007 an, dass die Sprachtests im März 2007 in den 9700 Kindertagesstätten (Kitas) bei etwa 180.000 Kindern gestartet werden. Das neue Schulgesetz sieht den Deutschtest zwei Jahre vor der Einschulung vor, um Sprachdefizite ermitteln und durch gezielte Förderung frühzeitig beseitigen zu können. Eine Grundschule soll künftig für jeweils drei Kindergärten Lehrer abstellen, die die Tests und später den Sprachunterricht abhalten zu können. Laschet: »Die Lehrer lernen schon früh ihr künftiges Schülerpotenzial kennen».

Durch ein »Filterverfahren» sollen die Sprachkenntnisse der Kinder in spielerischer Form und in Vierergruppen überprüft werden. Bei diesem »Grob-Screening« sind innerhalb von 25 Minuten im Rahmen eines eigens entwickelten Zoo-Spiels Aufgaben zu lösen, z.B. Sätze und Kunstwörter nachzusprechen. Bei erkennbaren Lücken müssen sich die Kinder einem zweiten individuellen Deutschtest stellen. Bei diesem 35-minütigen »Fein-Screening« sollen gezielte Förderempfehlungen abgeleitet werden. Der »Delfin4« genannte Test ist im Auftrag von NRW-Schulministerin Barbara Sommer (CDU) von WissenschaftlerInnen der Universität Dortmund entwickelt worden. Das Verfahren ist auch für die Vierjährigen vorgeschrieben, die keinen Kindergarten besuchen. Im Land sind es ca. 25.000 Kinder, die zunächst eine Aufforderung zum Sprachtests erhalten.

Bei den insgesamt 180.000 zu testenden Kindern rechnet das Düsseldorfer Schulministerium mit einer Quote von 20-25%, die eine spezielle Sprachförderung benötigen. Dieser Vorschulunterricht ist künftig ebenfalls verpflichtend und soll in den Kindergärten erteilt werden. Für die Sprachförderung eines Kindes werden die Kitas laut Laschet pro Jahr einen Landeszuschuss von 350 Euro erhalten, um hierfür externe Fachkräfte beschäftigen zu können. Die Mittel für die Sprachförderung sollen im Haushalt von derzeit 17 Mio. Euro bis zum Jahr 2010 auf 28 Mio. Euro erhöht werden. Die Einführung des Deutschtests wird nach Einschätzung von Laschet »einen Schub von Neuanmeldungen für die Kindergärten bringen«. Derzeit besuche ein Viertel aller Vierjährigen im Land noch keine Kita. Landesschulministerin Barbara Sommer (CDU) erklärte, »sprachliche Verarmung, mangelndes Ausdrucksvermögen und fehlendes Sprachverständnis« seien vor allem bei Kindern aus sozial benachteiligten Familien »eine Bildungsbarriere» (vgl. S. 22, 24; Nitschmann SZ 13.02.2007, 6; Der Spiegel 7/2007, 22).

Saarland

Geplante Verschärfung des Polizeigesetzes stößt auf Widerstand

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) hält einen Entwurf des saarländischen Innenministeriums für ein »Gesetz zur Erhöhung der inneren Sicherheit im Saarland« und die damit verknüpften Polizeigesetz-Änderungen für teilweise verfassungswidrig, insbesondere wegen des Vorhabens präventiver Telekommunikations-(TK-) Überwachung. »Konkrete Vorbereitungshandlungen für sich oder zusammen mit weiteren bestimmten Tatsachen« für das mögliche Begehen von Straftaten dürften nicht zur Rechtfertigung der TK-Überwachung genügen. Das Bundesverfassungsgericht habe der Legislative mit den richtungsweisenden Urteilen zum großen Lauschangriff (vgl. DANA 1/2004, 36) oder zur vorbeugenden Telefonüberwachung im niedersächsischen Polizeigesetz deutliche Grenzen gesetzt, die sich der saarländische Entwurf einzuhalten nicht die Mühe mache. Es werde zudem offen gelassen, ob die Ermittler entsprechende Maßnahmen selbst durchführen oder sich dabei eines Netzbetreibers bedienen wollen. Nicht klargestellt sei, ob die Überwachung auch mit den umstrittenen »IMSI-Catcher mit zusätzlicher Abhörfunktionalität« erlaubt sein soll.

Kritisiert wird, dass eine vorsorglich zu überwachende Person einen Anschluss lediglich »mit hoher Wahrscheinlichkeit« nutzen müsse. Der Kreis der besonders geschützten Vertrauensverhältnisse von »Geheimnisträgern« werde zudem »ohne erkennbaren Grund« enger gezogen als in vergleichbaren Regelungen anderer Bundesländer. Dorn im Auge ist auch die Pflicht von Mobilfunkunternehmen, den Polizeibehörden Auskunft über Geräte- und Kartennummern (IMEI, IMSI) und sogar von »Berechtigungskennungen« zu geben. Kritisiert werden weiterhin: Art, Umfang und

Dauer der Maßnahme sowie die tragenden Erkenntnisse und Begründungen für die Gefahr und die Verhältnismäßigkeit müssten nicht angegeben werden. Mit einer maximalen Dauer von drei Monaten, die sich auch auf Eilanordnungen beziehe, sei die zeitliche Obergrenze unverhältnismäßig hoch bemessen. Die Personenortung würde »jedem Polizeibeamten ermöglichen, ohne weitere Kontrolle unbegrenzt in das Fernmeldegeheimnis einzugreifen.« Anordnungen der Behördenleitung dürften unbegrenzt weiter nach unten delegiert werden. Die Benachrichtigungspflichten gegenüber Betroffenen seien zu lax.

Gegen den Entwurf hatte zuvor schon der saarländiche Datenschutzbeauftragte Roland Lorenz Position bezogen (DANA 2/2006, 88). Bei ihm lösten auch die vorgesehenen Befugnisse zur »anlassfreien elektronischen Erfassung von Kfz-Kennzeichen« und zur Ausweitung der Videoüberwachung Protest aus (Krempl www.heise.de 22.01.2007).

Sachsen-Anhalt

Auswertung von Kreditkartendaten gegen Internet-Pornografie

Anfang 2007 gelang Strafverfolgern bundesweit ein Schlag gegen Kinderpornografie im Internet; es wurden bundesweit Hunderte Wohnungen und Geschäftsräume durchsucht. Die Aktion basierte auf der Auswertung des gesamten Kreditkarten-Datenbestands Deutschlands mit mehr als 22 Mio. Datensätzen. Um die Konsumenten einer einschlägigen Seite im Internet zu ermitteln, ließen die Fahnder im Sommer 2006 den Zahlungsverkehr aller Kreditkartenbesitzer daraufhin überprüfen, ob eine Summe von 79,99 US-Dollar in einem festgelegten Zeitraum von 20 Tagen auf ein verdächtiges Auslandskonto überwiesen worden ist. Insgesamt wurden von den Ermittlern fünf Merkmale vorgegeben. Sämtliche um Auskunft ersuchten 14 Unternehmen der Kreditkartenwirtschaft kooperierten und gaben die Daten der verdächtigten Kunden preis. Die Entgeltzahlung war ausschließlich per Kreditkarte (Visa oder Master Card) möglich. Nach Angaben des Innenministers des Landes Sachsen-Anhalt Holger Hövelmann (SPD) hatten weder das Landeskriminalamt (LKA) noch die Staatsanwaltschaft Halle (Saale) unter der Leitung von Peter Vogt direkten Zugriff auf die Daten. Ein Sprecher des LKA bekräftigte, es habe sich um »ganz normale Ermittlungsmethoden« gehandelt. Die Justizministerin Angela Kolb (SPD) beteuerte, von Rasterfahndung könne hier keine Rede sein. Bei Vorliegen der genannten Eigenschaften habe eine ziemlich hohe Wahrscheinlichkeit bestanden, dass Kreditkartenbesitzer mit einer solchen Buchung auf der Abrechnung Kunden des Kinderporno-Portals gewesen sind.

Die Operation »Mikado« führte zu 322 Beschuldigten in Deutschland. Tatsächlich soll der größte Teil der 322 ermittelten Personen einschlägig vorbestraft oder zumindest polizeibekannt gewesen sein. Die Verdächtigten zeigten sich weitgehend geständig. Sie müssen, nachdem bei ihnen Durchsuchungen durchgeführt worden sind, nicht nur mit Strafverfahren rechnen, sondern nach den Allgemeinen Geschäftsbedingungen der Kreditkartenwirtschaft auch mit dem Verlust ihres Zahlungsmittels. Nach den Anbietern der Seite wird in Zusammenarbeit mit internationalen Behörden weiter gefahndet. Die Spur endete vorläufig bei einem Unternehmen auf den Philippinnen.

Der Landesbeauftragte für Datenschutz in Schleswig-Holstein Thilo Weichert vertrat die Ansicht, dass es sich hier um eine klassische Fahndungsmethode gehandelt habe, die im Grundsatz rechtlich nicht zu beanstanden sei. Sein Kollege von Sachsen-Anhalt Harald von Bose bestätigte, dass es nicht darum gegangen sei, sämtliche Finanztransaktionen aller deutschen Kreditkarteninhaber zu überprüfen, sondern um die »Namhaftmachung« eines überschaubaren Personenkreises.

Der Düsseldorfer Rechtsanwalt Udo Vetter ließ dagegen an dem Vorgehen der Strafverfolger kein gutes Haar. Für die Ermittlungsmaßnahme habe kein hinreichender Anfangsverdacht bestanden, da die Staatsanwaltschaft nur von der Existenz eines Kinderporno-Angebotes erfahren habe. Es bestehe eine Verpflichtung zur Datenherausgabe nach der Regelung zur Rasterfahndung (§ 98a StPO) nur bei richterlicher Anordnung. Auch wenn die Strafverfolger die Daten nicht selbst durchforsteten, hätten sie die Unternehmen unter Druck gesetzt und dadurch die Daten erlangt. Tatsächlich hatte die Staatsanwaltschaft fälschlich gegenüber den Unternehmen behauptet, dass diese sich gegebenenfalls strafbar machten, wenn sie nicht mitwirkten. Innerhalb von wenigen Tagen gingen mindestens 20 Beschwerden gegen die Aktion bei Gericht ein. Gegen die Ermittler und ein Durchsuchungen begleitendes Presseteam wurden zudem Strafanzeigen erstattet (Todt www.spiegel.de 08.01.2007; www.heise.de 08.01.2007 u. 09.01.2007; Todt www.spiegel.de 09.01.2007; PM MdI u. MJ Sachsen-Anhalt 09.01.2007; Kleinz www.heise.de 10.01.2007; Telepolis www.heise.de 15.01.2007; www.heise.de 29.01.2007; www.mikado-fahndung.de).

Sachsen

Datenschutzbeauftragter jetzt auch für den nichtöffentlichen Bereich zuständig

Der Sächsische Landtag hat dem Sächsischen Datenschutzbeauftragten (SächsDSB) mit Wirkung vom 01.01.2007 die bisher bei den vier Regierungspräsidien angesiedelte Zuständigkeit für die Datenschutzaufsicht im nichtöffentlichen Bereich gesetzlich übertragen. Der SächsDSB nimmt somit umfassend die Kontrolle des »Datenschutzes aus einer Hand« wahr. Eine weitere Änderung des Datenschutzgesetzes liegt darin, dass alle von der öffentlichen Hand beherrschten privatrechtlichen Unternehmen, die am Wettbewerb teilnehmen, die Daten ihrer KundInnen nach dem Bundesdatenschutzgesetz (BDSG) verarbeiten dürfen.

Die Novelle enthält zahlreiche weitere datenschutzorganisatorische Verbesserungen. So wird u.a. das Prinzip der Datenvermeidung und Datensparsamkeit in Sachsen erstmals gesetzlich verankert (PM SächsDSB 18.12.2006).

Ausländische Datenschutznachrichten

Niederlande
Audio- ergänzt Videoüberwachung

Die Firma Soundintellingence in Groningen/Niederlande hat als Spinoff die von Tjeerd Andringa und Peter van Hengel am Institut für Künstliche Intelligenz der Universität von Groningen entwickelte Überwachungssoftware »Slgard« serienreif gemacht. Mit ihr soll, i.d.R. in Ergänzung zu Videoüberwachung, akustisch »dicke Luft« detektiert werden. Das Programm ist dem Frühwarnsystem von Menschen nachempfunden, die anhand von angehobener, aggressiver Stimmen aufmerksam werden und erkennen, dass gleich etwas Ernstes passiert. Die damit ausgerüsteten Überwachungskameras schlagen nur Alarm, sobald in ihrem Umkreis ein Streit akustisch erkannt wird. Die Lauschkameras werden in Groningen, in Rotterdam und in Zügen installiert. Bei ersten Tests soll es bereits zu drei Festnahmen gekommen sein. Ob die erhobenen Stimmen wirklich auf eine drohende Keilerei hindeuten oder nur betrunkenes Gegröle sind, muss (noch) von einem Menschen entschieden werden. Die Technik soll sogar bei Discothekenlautstärke noch funktionieren. Wahrscheinlich wird aber künftig weiterhin der Einsatz v.a. in Fußgängerzonen erfolgen (Roth Telepolis www.heise.de 28.11.2006).

Großbritannien
Datenaustausch zwischen Behörden soll erleichtert werden

Der britische Premierminister Tony Blair gab bekannt, dass der Datenaustausch über BürgerInnen zwischen den Behörden erleichtert werden soll. Nachdem diese Ankündigung viel Staub aufgewirbelt hatte, sah sich Gesundheitsminister John Hutton veranlasst zu beschwichtigen, die Pläne seien keine weiteren Schritte in Richtung Überwachungsstaat. Die Regierung wolle keine »riesige Datenbank« oder ein neues IT-System einrichten. Es gehe vielmehr darum, bürokratische Hürden zu beseitigen. Bei den Behörden würden bereits Unmengen von Daten gespeichert, doch nicht zum Vorteil der BürgerInnen genutzt. Z.B. müsse eine Familie rund 40mal Kontakt mit den Behörden aufnehmen, um Formalitäten zu erledigen, wenn ein Angehöriger bei einem Verkehrsunfall stirbt. Das Department of Constitutional Affairs (DCA) ergänzte, die Bekämpfung von Identitätsdiebstahl solle verbessert werden, Bedürftigen könne besser geholfen werden und die Kommunikation von Unternehmen mit Behörden werde entbürokratisiert. Der bisher schon mögliche Datenaustausch habe z.B. geholfen, soziale Brennpunkte auszumachen.

Die Opposition von Konservativen und liberalen Demokraten verdächtigt dagegen die Regierung, die BürgerInnen ausschnüffeln zu wollen. Der Konservative Oliver Heald kritisierte, die Regierung versuche schrittweise z.B. mit Hilfe von Projekten wie einer Kinderschutz-Datenbank, über jeden britischen Einwohner möglichst viele Daten zu sammeln. Die Regierenden der Labour Party seien respektlos gegenüber der Privatsphäre der BürgerInnen.

Ein weiteres Regierungsprojekt sieht die Aufzeichnung sämtlicher Verkehrsbewegungen vor. In der nationalen DNA-Datenbank werden inzwischen die genetischen Daten von 3,5 Mio. Menschen gespeichert. Die Behörden verfügen über die Fingerabdrücke von rund 6 Mio. Menschen. Der britische Datenschützer Richard Thomas forderte in einem offiziellen Bericht im November 2006 vor diesem Hintergrund ein Umdenken bei der Überwachung. BürgerrechtlerInnen der Organisation No2ID vermuten, dass die geplante Einführung einer ID-Karte in Großbritannien nur ein Vorwand ist, um eine nationale Datenbank einzurichten. Im Dezember 2006 hat die britische Regierung vorläufig Pläne für ein neues Computersystem für die Verwaltung im Zusammenhang mit der ID-Karten-Einführung fallen gelassen. Das Projekt hätte nach Schätzungen der Opposition 20 Milliarden Pfund (30 Mrd. Euro) gekostet. Die Pläne zur Überarbeitung der Richtlinien für den Datenaustausch zwischen den Behörden soll nun in einem Gremium beraten werden, dem 100 BürgerInnen angehören und das Anfang März 2007 eine Stellungnahme abgeben soll (www.heise.de 15.01.2007).

Großbritannien
Haftstrafen für Datenschutzverstöße

Der Diebstahl von und der illegale Handel mit privaten Daten soll nach Plänen des britischen Justizministeriums künftig schärfer bestraft werden. Gemäß dem Entwurf einer Änderung des Datenschutzgesetzes sollen der Handel und der vorsätzliche Missbrauch persönlicher Daten Dritter mit bis zu zwei Jahren Haft bestraft werden können. Der Data Protection Act (DPA) von 1998 sieht lediglich Geldstrafen vor. Nach einer Mitteilung des Ministeriums ist die britische Regierung zunehmend besorgt über das offensichtliche Wachstum des Handels mit persönlichen Daten. Der DPA wirke nicht mehr ausreichend abschreckend. Justizminister Charles Falconer: »Die Leute haben ein Recht darauf, dass ihre Privatsphäre vor mutwilligem Missbrauch geschützt werden, Der Datenaustausch innerhalb der öffentlichen Verwaltung kann für die Bevölkerung von großem Nutzen sein und ist vereinbar mit einem angemessenen Schutz der individuellen Privatsphäre. Ein wesentliches Mittel, diese Vereinbarkeit zu erhalten, ist die Sicherheit und Integrität dieser Daten zu gewährleisten« (www.heise.de 08.02.2007).

Großbritannien
Entkleidende Beobachtung mit Terahertz-Durchleuchtung

Gemäß einem Bericht der Boulevard-Zeitung »The Sun« plant das britische Innenministerium den Einbau von Durchleuchtungskameras in Straßenlaternen, um mit einer Spezialtechnik durch die Kleidung der Menschen sehen zu können. Gemäß einem zitierten

internen Schreiben vom 17.01.2007 heißt es: »Die Entdeckung von Waffen und Sprengstoff wird einfacher«. Mit Hilfe von sog. Terahertz-Strahlung, die von »Straßenmobiliar« wie z.B. Straßenlaternen, Mülleimern und Parkbänken ausgestrahlt werde, könnten Materialien wie Textilien oder bestimmte Kunststoffe durchdrungen werden. Mit Scannern, wie sie z.B. vom britischen Sicherheitsunternehmen Qinetiq hergestellt werden, könnten versteckte Risiken erkannt werden. An Flughäfen wird die Technik schon seit einiger Zeit eingesetzt, was bei den Fluggästen auf Kritik stieß, weil diese sich von Sicherheitsbeamten z.B. nicht unter den BH schauen lassen wollten. Inzwischen wurde geklärt, dass solche Untersuchungen nur mit Einwilligung der Durchleuchteten erlaubt sind. Ein weiterer kritisierter bisheriger Einsatzbereich ist die Heranziehung solcher Geräte durch die Polizei, z.B. um bei Razzien im Rotlichtmilieu am Körper versteckte Drogen aufzufinden. Demgemäß sorgen sich die Staatsschützer aus dem britischen Innenministerium, dass die »soziale Akzeptanz« ein »begrenzender Faktor« sein könne. Die Privatsphäre sei »ein Thema«, weil »die Maschinen durch Kleidung hindurchsehen«. Man könne aber darüber nachdenken, Aufnahmen weiblicher Überwachter nur von Frauen sichten zu lassen. Dies jedoch sei bei größeren Menschenmengen »sehr problematisch« (vgl. DANA 1/2004, 27; www.spiegel.de 29.01.2007; www.heise.de 29.01.2007).

Großbritannien

Kreditkartendaten mit MP3-Player abgefangen

Ein Betrügerring hat in England mit Hilfe von handelsüblichen MP3-Playern Kreditkartendaten abgefangen, indem er sich mit den Geräten zwischen die Telefondose und Bankterminals einklinkte und die Datenübertragungen aufzeichnete. Diese kriminelle Methode soll aus Malaysia stammen. Die betroffenen Bankterminals waren in Kneipen, Bingohallen und Bowling-Centern aufgestellt und mit einem Stecker in einer Telefondose verbunden. Zwischen dem Stecker und der Dose platzierten die Kriminellen einen Zweiwege-Adapter, an den sie die MP3-Player anschlossen. Die aufgezeichneten Modem-Datenübertragungen entschlüsselten sie mit einem sog. Modem Line Tap aus Kanada, der regulär zum Mitschneiden und zum Debuggen von Modem-Verbindungen dient, bzw. mit einer Software aus Russland. Mit dem Wissen über Kreditkartensysteme war es dem Kopf der Bande – einem Maxwel Parsons – möglich, die Kreditkartennummern und deren Ablaufdaten zu rekonstruieren. Diese Daten wurden zum Klonen von Kreditkarten genutzt, mit denen Waren im Wert von ca. 200.000 Pfund auf fremde Rechnung gekauft wurden.

Parsons war zufällig geschnappt worden, weil im Rahmen einer Kfz-Kontrolle wegen falschen Abbiegens in seinem Auto eine gefälschte Kreditkarte gefunden wurde. Bei der anschließenden Wohnungsdurchsuchung fanden die Beamten die technische Ausrüstung der Fälscher sowie 18 geklonte und acht gefälschte Kreditkarten. Als Gegenmaßnahmen will die britische Kreditwirtschaft jetzt mit PIN geschützte Chipkarten einführen. Dies würde aber nichts daran ändern, dass Kreditkartenzahlungen über das Internet immer noch für einen solchen Angriff anfällig blieben. Die Schutzmaßnahmen für den elektronischen Zahlungsverkehr sind in Großbritannien bisher weit lockerer als in Deutschland, wo eine solche Betrugsmethode scheinbar nicht möglich wäre (www.heise.de 20.11.2006).

Großbritannien

Handflächen-Scanning in der Schule

Eine schottische Grundschule in Paisley bei Glasgow hat für eine Vielzahl von Aktivitäten die biometrische Identifikation eingeführt. Die Kinder dort bezahlen für ihr Mittagessen nicht mehr mit Geld, Gutscheinen oder Chipkarten, sondern indem sie eine Hand vor einen Handflächenscanner halten. Gemäß Herstellerangaben bietet das Verfahren mehr Sicherheit als die Analyse eines Fingerabdrucks. Das Gerät ermittelt das unverfälschbare Muster der Blutgefäße in der Hand und vergleicht es mit dem Datenbestand. Der angeschlossene Computer wickelt nicht nur die Bezahlvorgänge ab, sondern prüft auch, ob die Kinder bekannte Lebensmittelallergien gegen die von ihnen gewählten Speisen haben. Das System soll künftig auch eingesetzt werden, um morgens die Anwesenheit zu kontrollieren, Fremde am Zugang zur Schule zu hindern oder festzuhalten, wer welche Bücher aus der Schulbücherei ausgeliehen hat. Kritiker sehen in dem Projekt ein weiteres Beispiel für die wachsende elektronische Totalüberwachung. Den Kindern macht die Technik angeblich Spaß (Der Spiegel 45/2006, 173).

Großbritannien

Filmische Lebensdokumentation

Das britische Projekt »UP-Series« ist eine der längsten filmischen Dokumentationen in Europa. Es begann 1964 mit 14 Kindern unterschiedlicher Herkunft im Alter von jeweils sieben Jahren. Gezeigt werden sollte, wie viel Einfluss die Herkunft auf ihre Entwicklung haben würde. Alle sieben Jahre wurden die Ausgewählten wieder gefilmt und nach ihren Wünschen fürs Leben befragt. Seit 1970 ist der internationale erfolgreiche Spielfilmmacher Michael Apted Regisseur der Dokumentation; die UP-Series bezeichnet er als sein Hauptwerk. Von den vier Frauen und 10 Männern sind zwei Männer im Laufe der Zeit abgesprungen. Nun ist in England und in den USA der 7. Film als DVD herausgekommen. »49 UP« zeigt die Porträtierten im Alter von 49 Jahren und bestätigt die These, dass die Kinder aus privilegiertem Hause Karriere gemacht haben, nicht aber die Kinderheimzöglinge. Apted hatte das große Glück, Beweise für die erstarkende Mittelschicht zu finden und überraschende Lebenswege verfolgen zu können, so etwa die des begabten Jungen Neil, der in seinen Zwanzigern nach abgebrochenem Studium obdachlos wurde, schließlich Schritt für Schritt wieder zu Kräften kam und heute als Lokalpolitiker Ansehen genießt (Der Spiegel 2/2007, 43).

Italien

Bankraub mit abgetrenntem Finger

In Rom haben Bankräuber am 26.01.2007 die durch ein biometrisches System gesicherte Tür der Banco di Brescia mit einem abgetrennten menschlichen Finger geöffnet und bei ihrem Überfall 12.000 Euro erbeutet. Zahlreiche italienische Banken haben

mittlerweile einen Fingerabdruck-Scanner, den »Bio-Digit«, an der Eingangstür installiert. Die gescannten Fingerabdrücke werden im System gespeichert, um potenzielle Täter am Zutritt zu hindern bzw. abzuschrecken. Sie werden jedoch nicht automatisch mit einer Referenzdatenbank abgeglichen. Der bei dem Überfall verwendete Finger, der bei der Flucht der Täter zurückblieb, stammt vermutlich von einer Frau. Die Täter hatten ihn mit Eis »frisch gehalten«. Die Polizei sucht nun nach Leichen, denen ein Finger fehlt. Es war das erste Verbrechen dieser Art in Italien (Datenschutzberater – DSB 2/2007, 4; www.heise.de 29.01.2007).

Polen

Stasi-Informant wird nicht Bischof von Warschau

Am 07.01.2006, zwei Tage nach seiner formellen Amtsübernahme, wurde der 67jährige Kirchenmann Stanislaw Wielgus nicht als Bischof von Warschau in sein Amt eingeführt und damit nicht zu einer der wichtigsten Kirchenführer in dem zu gut 90% katholischen Polen. Dem Verzicht auf das Amt ging eine Debatte über die jahrzehntelangen Kontakte zur früheren kommunistischen Staatssicherheit SB (Sluzba Bezpieczenstwa) voraus. Gemäß veröffentlichten SB-Dokumenten hatte Wielgus nach längerem »Vorlauf« bei der SB 1973 von diesem Geheimdienst eine Schulung und den Auftrag erhalten, sich um ein Humboldt-Stipendium in München zu bemühen. Zunächst kam es aber offenbar zu keiner konkreten Zusammenarbeit. Später sollte Wielgus versuchen, in die Redaktion des nach Osteuropa sendenden Radio Free Europe in München einzutreten, was gemäß den Geheimdienstakten ein »Hornissennest« war. Der Versuch scheiterte. Hauptgrund für die Zusammenarbeit war offenbar der Wunsch des Kandidaten, wissenschaftlich Karriere zu machen.

Aus den Akten, die aus dem 1998 gegründeten polnischen Institut für nationale Erinnerung (IPN) stammen, geht hervor, dass »sein Vertrauen wuchs«. Wielgus »teilte den Mitarbeitern des SB immer freier seine eigene Sicht und Meinung mit«. In etwa 50 Begegnungen mit den SB-Offizieren im Laufe von etwa mehr als fünf Jahren habe er »eine Reihe konkreter Informationen« übermittelt. So soll er weitere Kandidaten für »operative Gespräche« an der Universität genannt, Charakteristiken von Priestern und Wissenschaftlern erstellt und über die Stimmung unter dem Lehrpersonal der Hochschule und den Gläubigen in Lublin während der politischen Krisen im März 1968 und Dezember 1970 berichtet haben. Er führte die Pseudonyme Grey, Adam und Adam Wysocki. Die Zusammenarbeit mit den Diensten soll bis Anfang 1990 gedauert haben. Als die ersten Vorwürfe gegen Wielgus laut wurden, hatte der Vatikan dem designierten Erzbischof zunächst eine Unbedenklichkeitsbescheinigung ausgestellt. Der Papst habe volles Vertrauen in den Kandidaten. Eine Geschichtskommission der polnischen Kirche war vorsichtiger, wenn sie feststellt, dass die Beweise für die »wissentlich und im Geheimen« geführte Zusammenarbeit des Herrn Wielgus »zahlreich« seien. Allerdings gebe es keinen Beweis, dass Wielgus jemandem tatsächlich geschadet habe. Wenige Tage vor dem Rückzug von Wielgus waren 68 Seiten seiner SB-Akte von der Wochenzeitung Gazeta Polska ins Internet gestellt worden. Wielgus selbst erklärte: »Ich habe niemanden ausspioniert. Ich habe weder in Worten noch in Taten Schaden angerichtet.« Es sei »falsch«, ihm üble Absichten oder schlechtes Verhalten gegenüber der Kirche zu unterstellen. Eine Vereinbarung zur Zusammenarbeit aus dem Jahre 1978 habe er vor einer Reise nach Deutschland unter Zwang unterschrieben.

Während zu dem Gottesdienst für die Amtseinführung am 07.01.2007 schon die Glocken läuteten, verlas der Sprecher der Erzdiözese im Fernsehen die Sätze: »Nach Artikel 2 Punkt 401 des kanonischen Rechtes hat Erzbischof Stanislaw Wielgus um die Entbindung von seinen Pflichten gebeten.« Papst Benedikt XVI. habe dieses Rücktrittsgesuch angenommen. In diesem Moment setzte vor der Kirche ein Platzregen ein und eine Stimme rief: »Es regnet, weil Gott weint!« Der erzkonservative polnische Ministerpräsident Kaczynski soll kurz zuvor den Papst persönlich angerufen und ihm dargelegt haben, welcher Schaden für Nation und Kirche entsteht, wenn ein überführter SB-Agent an der Spitze der Warschauer Kirche steht.

Die Amtskirche ist durch eine Welle von Stasi-Fällen im Jahr 2006 in Turbulenzen geraten (DANA 3/2006, 141). Konrad Hejmo, jahrzehntelang für die Betreuung polnischer Pilger im Vatikan zuständig, spitzelte für die Kommunisten ebenso wie Mieczyslaw Malinski, ein Kommilitone und Freund des verstorbenen Papstes Johannes Paul II. Ein anderer Michal Czajkowski, mit Verdiensten um die Annäherung zu den Juden, hatte dem SB über Jerzy Popieluszko Auskunft gegeben. Jener Pater war 1984 entführt, misshandelt und später tot in einem Stausee aufgefunden worden. Bis zu 15% der Priesterschaft, darunter zahlreiche Bischöfe – so schätzen Historiker – sollen mit dem Staat kooperiert haben. Mit Spannung wird ein im Jahr 2007 erscheinendes Buch des Krakauer Priesters Tadeusz Isakowicz-Zaleski erwartet, in dem dieser Stasi-Kontakte zahlreicher Krakauer Priester offenlegen will. Darin wirft er 39 Geistlichen aus der Region Krakau vor, für den SB spioniert zu haben. Ein neues Gesetz über die »Lustration« (Durchleuchtung) von Amtsträgern und die Aktenaufarbeitung, das dem deutschen Stasi-Unterlagengesetz entspricht, ist in Kraft getreten, in dem in vielen Fällen eine Umkehr der Beweislast vorgesehen ist. Dies bedeutet, dass bei bestimmten Positionen Stasi-Verdächtige ihre Unschuld beweisen müssen. Ein Tag nach dem Rücktritt von Wielgus ist erneut ein ranghoher Priester wegen seiner Geheimdienstkontakte zurückgetreten. Der Prälat der Wawel-Kathedrale in Krakau Janusz Bielanski bot Kardinal Stanislaw Dziwisz seinen Rücktritt an; dieser wurde sofort angenommen (Gnauck Die Welt 06.01.2007, 7; Kieler Nachrichten 06.01.2007, 4; Urban SZ 08.01.2007, 1, 3; Urban SZ 09.01.2007, 7; Puhl, Der Spiegel 3/2007, 110 f.).

Lettland

Deutsche Bundesdruckerei liefert Personalisierung für ePass

Die Berliner Bundesdruckerei International Services GmbH liefert für das lettische Innenministerium das komplette Personalisierungssystem zur Herstellung der neuen elektronischen Reisepässe. Der Auftrag hat ein vorläufiges Volumen im einstelligen Millionenbereich. Insgesamt wird Lettland in der Erstausstattung rund 1,1 Mio. neue Pässe herstellen. Das zum Einsatz kom-

mende Laser-Personalisierungssystem vom Typ Maurer ME500 soll weltweit das einzige System sein, mit dem sowohl biometrische Reisepässe als auch ID-Karten optisch und elektronisch personalisiert werden können. Das System soll auch für die Personalisierung der geplanten elektronischen ID-Karten in Lettland eingesetzt werden. Neben der Hardware-Ausstattung des Personalisierungszentrums in Riga liefert die Bundesdruckerei dem Office of Citizenship and Migration Affairs of the Ministry of Interior (OCMA) sämtliche notwendigen Software-Komponenten, die den Prozess zur zentralen Personalisierung sicherstellen. Darüber hinaus stellt das Unternehmen die erforderliche ICAO-konforme Public-Key-Infrastruktur (PKI) bereit. Die Auslieferung soll Sommer 2007 beginnen (Omnicard Newsletter Februar 2007, www.bundesdruckerei.de).

Bulgarien

Tod eines Geheimdienst-Archivars

Der Streit um die Öffnung von Geheimdienst-Akten aus der Zeit des Kommunismus hat in Bulgarien durch den Tod des obersten Geheimdienst-Archivars eine besondere Note bekommen. Während das Innenministerium und die Staatsanwaltschaft von einem Selbstmord sprachen und dafür persönliche Motive nannten, äußerte die Opposition den Verdacht, es gebe berufliche Gründe; selbst einen Mord wollte der konservative Parlamentsabgeordnete Atanas Atanassow, der selbst von 1997 bis 2001 den Nationalen Geheimdienst geleitet hatte, nicht ausschließen. Bei dem Toten handelt es sich um den 61jährigen Bozhidar Doytschew. Er war am 15.11.2006 an seinem Arbeitsplatz gefunden worden. Der Vorfall wurde erst zwei Tage später durch die Meldung eines in London ansässigen Internet-Dienstes bekannt, der sich auf EU-Quellen berief. Generalstaatsanwalt Boris Weltschew äußerte Verwunderung über diese Verzögerung, meinte aber, es gebe keine Zweifel an den persönlichen Motiven des Suizids. Ministerpräsident Sergej Stanischwe widersprach Vermutungen, die Nachricht sei bewusst zurückgehalten worden.

Das Parlament verhandelt derzeit zum wiederholten Mal ein Gesetz über die Öffnung der Archive der Staatssicherheit. Die EU-Kommission in Brüssel widmet diesem Entwurf im Vorfeld des bulgarischen EU-Beitritts besondere Aufmerksamkeit. Bulgarien ist eines der letzten vormals kommunistischen Länder, das erst jetzt die früheren Geheimdienstakten umfassend freigeben will. An die nun vorbereitete Öffnung der Archive werden seit langem Spekulationen geknüpft, ob hierdurch Untaten des früheren bulgarischen Geheimdienstes bekannt werden könnten. Diesem war z.B. eine Beteiligung an dem Attentat auf Papst Johannes Paul II in Rom im Jahr 1981 angelastet worden (Brill, SZ 22.11.2006, 8).

USA

Hunderte Millionen für Überwachung

Nach den Plänen von US-Präsident George W. Bush sollen im Haushaltsjahr 2007/2008 hunderte von Millionen US-Dollar für Überwachung und biometrische Personenerfassung ausgegeben werden. Allein 146,2 Mio. US-Dollar sind für neue Geräte vorgesehen, mit denen an den Grenzen künftig alle zehn Finger einer einreisenden Person digital eingescannt und gespeichert werden können. Bislang erfassen die Behörden lediglich die Fingerlinien der beiden Zeigefinger. Das umstrittene Flugpassagier-Screening-Programm Secure Flight soll 2007 mit zusätzlichen 38 Mio. US-Dollar ausgestattet werden. Eine Milliarde US-Dollar ist für die sog. Secure Border Initiative des Department of Homeland Security (DHS) eingeplant, mit dem v.a. die Grenze zu Mexiko, aber auch die zu Kanada, gesichert und der Strom illegaler EinwanderInnen eingedämmt werden soll. Ziel ist die Installation eines »virtuellen Zauns«, der mit Hightech-Elektronik ausgestattet ist – von hochsensiblen Bewegungssensoren über Infrarotkameras bis hin zum Einsatz von Unmanned Aerial Vehicles (UAV) und Drohnen. Den Auftrag zur Errichtung des virtuellen Zauns hatte 2006 ein Konsortium um den Flugzeug- und Rüstungskonzern Boing zugesprochen bekommen.

Für die Entwicklung neuer Sicherheits- und Überwachungstechniken sollen dem DHS allein im Jahr 2008 insgesamt 800 Mio. US-Dollar zur Verfügung stehen. Programme des Justizministeriums zur »Verhinderung und Bekämpfung terroristischer Aktivitäten« sollen mit zusätzlichen 227 Mio. US-Dollars gefördert werden, darunter 37,8 Mio. US-Dollar für den Bedarf, »Daten in öffentlichen und privaten Netzwerken sicher überwachen zu können«, sowie 22,8 Mio. US-Dollar für Aktivitäten auf dem Gebiet der Computeranalyse und der digitalen Forensik. Knapp 119 Mio. US-Dollar soll das Justizministerium für die Verfolgung von Straftaten im Bereich der Internet-Kinderpornografie erhalten (www.heise.de 06.02.2007).

USA

Sicherheitsgefahr durch Web-Cam im Strafvollzug

Der Sheriff im Bezirksgefängnis von Anderson im US-Staat Tennessee hat eine Web-Cam installiert, um der Öffentlichkeit zu zeigen, wie es dort so zugeht und um die Menschen zu rechtskonformen Verhalten anzuhalten. Die Kamera zeigte ein Kontrollpult der Gefängniswärter, man konnte die Flurtüren sehen, und manchmal gab es vor der Web-Cam sogar eine kleine Schlägerei unter Gefangenen. Über sechs Jahre lang war das Angebot im Internet und wurde von mehr als einer Million Surfern angeklickt. Nun stellte sich heraus, dass manche Zuschauer die Einblicke nutzten, um Drogen in das Gefängnis zu schmuggeln. Sie hatten die Dienstpläne der Wärter genau protokolliert, sie wussten, wann Gefangenentransporte stattfanden und konnten sich ausrechnen, wann ein Schmuggelversuch besonders erfolgversprechend sein würde. Andere machten sich einen Spaß daraus, die Wärterinnen abzupassen, sie im Kontrollraum anzurufen und am Telefon zu belästigen. Im November 2006 schaltete Sheriff Paul White die Web-Cam ab (Der Spiegel 49/2006, 71).

USA

WählerInnen für lebenslange GPS-Kontrolle von Sexualtätern

Parallel zu den Wahlen in den USA Anfang November 2006 wurde in verschiedenen Staaten über einzelne Gesetze abgestimmt, so auch in Kalifornien über den Gesetzesvorschlag Nr. 83,

der Sexualstraftäter lebenslang verpflichtet, ein GPS-System zu tragen. 70% der WählerInnen stimmten dem Gesetz, das eine Verschärfung eines schon in Florida geltenden Gesetzes ist, zu. In Kalifornien gibt es ca. 90.000 Sexualstraftäter, die sich bei lokalen Behörden melden müssen. Ihre Namen werden mit zahlreichen persönlichen Daten auf einer Webseite veröffentlicht (zu Deutschland und mit vielen Nachweisen DANA 4/2006, 169). Das neue Gesetz verschärft die zu verhängenden Strafen und verpflichtet Sexualstraftäter lebenslang zu noch größeren Entfernungen zwischen der eigenen Wohnung und Schulen, Parks oder Kinderspielplätzen. Sexualstraftäter, die einmal eine Gefängnisstrafe verbüßt haben, müssen nicht nur während der Bewährungszeit, sondern lebenslang ein GPS-System mit sich führen. Welche Technik eingesetzt wird, ist noch nicht klar. Möglich ist eine kostengünstigere passive Überwachungslösung oder eine teurere aktive Dauer-Kontrolle in Echtzeit (www.heise.de 09.11.2006; vgl. zu Großbritannien DANA 3/2006, 140).

USA

Bob Dylan gegen Filmfalschdarstellung

Kurz bevor der Films »Factory Girl« Ende 2006 in die Kinos kam, forderte US-Folk-Legende Bob Dylan vom Drehbuchautor und Produzenten Vertrieb und alle Vorschauen des Films einzustellen, bis er den Film gesehen hat. Er befürchtete darin verunglimpft zu werden. Der Film handelt vom Suizid der Andy-Warhol-Muse Edie Sedgwick. Durch die Darstellung der Ereignisse fühlt sich Dylan hierfür verantwortlich gemacht. Edie Sedgwick war Fotomodell und It-Girl und galt als Stil-Ikone der 60er Jahre. 1971 kam sie durch eine Überdosis Schlafmittel ums Leben. In der Verfilmung ihrer tragischen Lebensgeschichte heißt der Mann, der sie verlässt und damit in die Drogensucht und den Suizid treibt, zwar Danny Quinn. Doch wird er mit Mundharmonika und Kappe dargestellt, die untrüglichen Markenzeichen von »His Bobness« Dylan.

Die Anwälte von Dylan schrieben an die Filmverantwortlichen: »Sie scheinen unter dem Missverständnis zu leiden, dass allein die Änderung des Namens ... Sie vor einer Klage bewahrt.« Die Darstellung sei verunglimpfend und verletze das Persönlichkeitsrecht von Dylan (SZ 16./17.12.2006, 24).

USA

Pentagon und CIA forschen im Inland Konten aus

Das US-Verteidigungsministerium hat auf Grund einer weitgehend unbekannten Regelung innerhalb der USA Finanzdaten von Hunderten Spionage- und Terrorismusverdächtigen erhoben. Gemäß Presseberichten erklärte ein Mitarbeiter des Ministeriums inoffiziell, dieses Vorgehen sei Teil einer aggressiven Ausdehnung der Armee in nachrichtendienstliche Tätigkeiten im Inland. Der Auslandsnachrichtendienst CIA, der wie die Armee im Inland ebenfalls bei der nachrichtendienstlichen Tätigkeit strengen Beschränkungen unterliegt, habe ebenfalls – allerdings in wenigen Fällen – solche Daten erhoben. Selbst führenden Beamten war es unbekannt, dass das Ministerium und die CIA mit eigenen Formularen Banken, Kreditkartengesellschaften und andere Unternehmen in der Finanzbranche um freiwillige Auskünfte gebeten hätten (SZ 15.01.2007, 8).

USA

Hersteller zu 10 Jahre Datenschutzaudit verpflichtet

Das US-amerikanische Forensik-Unternehmen Guidance war im Dezember 2005 Opfer eines Servereinbruchs geworden, bei dem Namen, Adressen und Kreditkartendaten von rund 3800 Kundinnen und Kunden kopiert wurden. Als Reaktion hierauf verpflichtete nun die U.S. Federal Trade Commission (FTC) das Unternehmen zu höheren Sicherheitsmaßnahmen. Die Einbrecher hatten für den Datenzugriff eine SQL-Injection-Schwachstelle genutzt. Nach Ansicht von FTC hatte es Guidance versäumt, ausreichend Vorkehrungen zum Schutz der Kundendaten zu treffen. Diese Art von Schwachstelle und wie man sich insofern schützt sei hinreichend bekannt. Das Unternehmen hätte mit Angriffen auf Webanwendungen rechnen müssen. Erschwerend bei der Beurteilung des Falles wertete die FTC, dass Guidance auf seinen Webseiten vollmundig die Sicherheit von Kundendaten anpries – und sie dennoch im Klartext abspeicherte. FTC verpflichtete den Hersteller der Forensik-Software Encase zur Implementierung eines umfassenden Cybersecurity-Programms und dazu, den Erfolg seiner Bemühungen zehn Jahre lang von unabhängigen Sicherheitsauditoren überprüfen zu lassen. Die FTC schloss damit ihren 14. Fall von Datenschutzverletzungen durch US-Unternehmen ab.

In Deutschland werden derartige Datenschutzvergehen regelmäßig nicht geahndet. Firmen sehen sich nicht veranlasst, ihre Kundinnen und Kunden über erfolgreiche Angriffe zu informieren. Dem gegenüber gelten z.B. im US-Bundesstaat Kalifornien strenge Richtlinien: Der Security Breach Information Act zwingt Unternehmen zur Meldung von Einbrüchen in ihr System, wenn dort personenbezogene Daten verarbeitet werden. Einen ansatzweise ähnlichen Ansatz versucht die EU-Kommission auf den Weg zu bringen. Danach sollen zumindest Netzbetreiber und Internet Service Provider verpflichtet werden, Attacken gegen ihre Systeme der Regulierungsbehörde mitzuteilen, die dann über eine Benachrichtigung der Öffentlichkeit entscheidet (www.heise.de 17.11.2006).

Iran

Registrierungspflicht aller Webseitenbetreiber

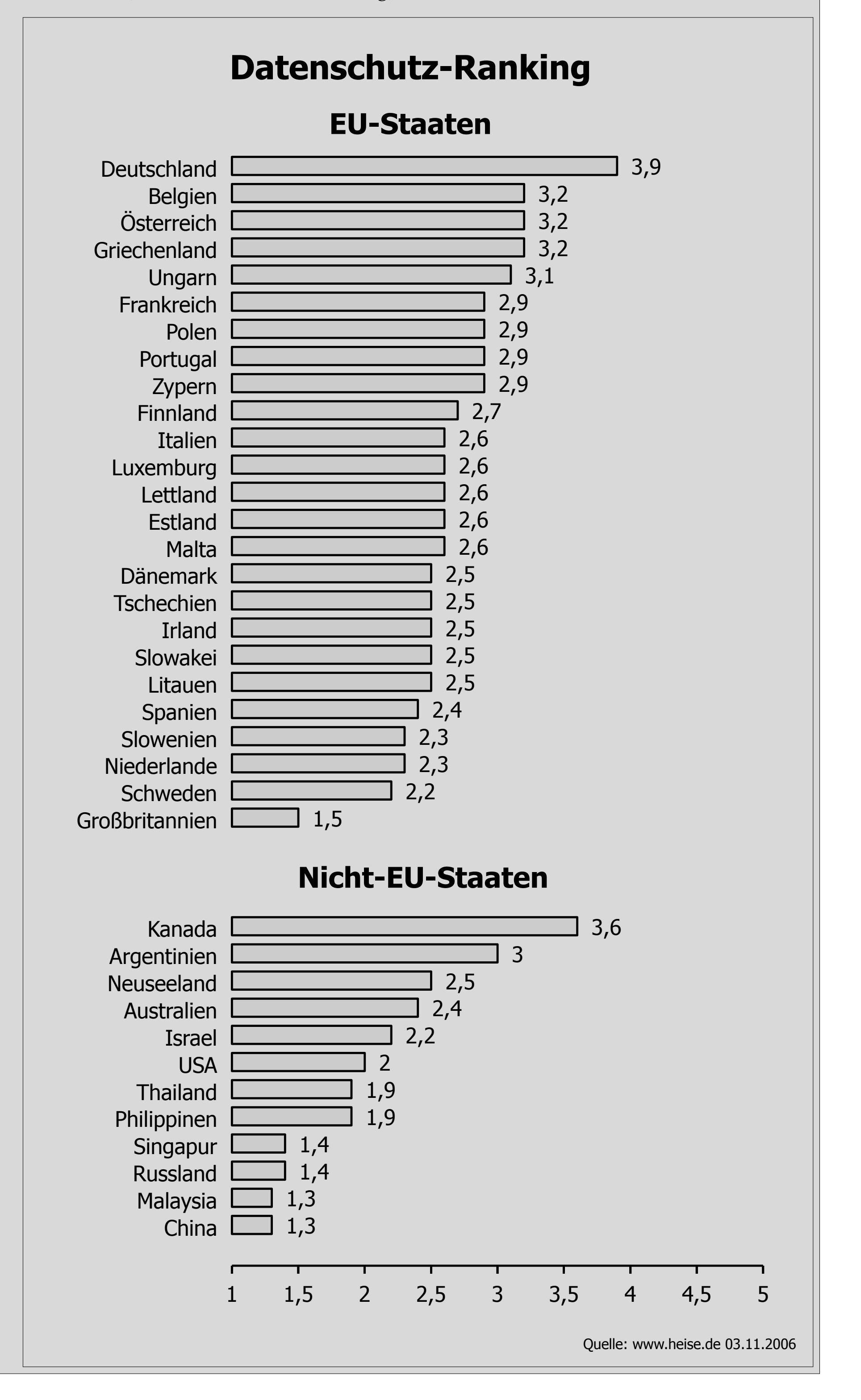
Die Regierung des Iran versucht, ihre Kontrolle über das Internet auszuweiten. Januar 2007 trat eine Regelung in Kraft, wonach sich Webseiten-Betreiber und Blogger auf einer Regierungswebseite mit Namen und Adresse registrieren lassen müssen. Beschlossen wurde dies nicht vom Parlament, sondern direkt vom Kabinett des Präsidenten Ahmadinedschad. Die Erfassung soll dem Zweck dienen, religiöse und kulturelle Werte zu bewahren und »zivile wie legale Verantwortlichkeiten« zu schaffen. Damit erfolgt die zweite Restriktion der Internetnutzung im Iran. Vor dem Jahreswechsel gab es eine staatliche Anordnung an alle iranischen Internet-Anbieter, die Bandbreite der Anschlüsse drastisch zu begrenzen. Damit sollte das Herunterladen von als gefährlich eingeschätzter Musik, eben-

International

Privacy International veröffentlicht Datenschutz-Ranking

Großbritannien gilt im jüngsten der jährlich herausgegebenen Berichte der Bürgerrechtsorganisation Privacy International als weltweit führende Überwachungsgesellschaft. Für den Bericht 2006 wurde versucht, den Stand des Datenschutzes und der Überwachung in 70 Ländern zu erfassen. Der Bericht hält fest, dass in vielen Ländern, legitimiert durch den Kampf gegen den Terrorismus, die Überwachung aus- und der Datenschutz abgebaut wurden. Genannt werden u.a. biometrische Pässe, Datenbanken und Kontrollen, Überwachung der Kommunikation, längere Datenspeicherungen, Austausch der Informationen mit anderen Behörden und Staaten, Auslagerung der Überwachung an private Firmen, Videoüberwachung und Data-Mining. Zur staatlichen Überwachung kommt die Privatwirtschaft, die zunehmend mehr persönliche Daten sammelt. Hervorgehoben wird hier v.a. die Verbreitung von RFID-Chips in allen Bereichen, mit denen sich z.B. KonsumentInnen leichter überwachen lassen. Der Bericht weist auch darauf hin, dass in vielen Ländern DatenschützerInnen und Bürgerrechtsorganisationen aktiv sind und auch manche Erfolge erzielt haben.

Im Vergleich der Länder schneidet Großbritannien unter den westlichen Demokratien am schlechtesten ab und steht als »endemische Überwachungsgesellschaft« auf gleicher Stufe mit Russland, China, Malaysia und Singapur. Mit einer Vielzahl von neuen Gesetzen wurde in allen Bereichen die Überwachung in den vergangenen Jahren »exzessiv« ausgebaut. Lobend erwähnt wird hingegen das Informationsfreiheitsgesetz. Bei den EU-Staaten steht, was den Datenschutz anbelangt, Deutschland an erster Stelle. Belgien, Österreich, Griechenland und Ungarn folgen auf den Plätzen. Die Bestnote – durchgehende Einhaltung von Menschenrechten und keine invasive Politik – erhielt kein Land. Vor Großbritannien mit dem schlechtesten Datenschutz rangieren in Europa Spanien, Slowenien, die Niederlande und Schweden. Bei den außereuropäischen Ländern schneiden Kanada und Australien am besten ab. Die USA stehen gleichauf mit Thailand und den Philippinen als »umfassende Überwachungsgesellschaften». Bei dem Scoring wurden Noten von 1 (endemische Überwachung) bis 5 (konsistente Beachtung menschenrechtlicher Standards) in 13 Kategorien vergeben. (www.heise.de 03.11.2006).



solchen Videos oder Fernsehprogrammen aus dem Ausland erschwert werden (Der Spiegel 2/2007, 43).

Singapur

Citibank führt Biometrie-Bezahlsystem ein

Die Citibank, weltweit größter Finanzdienstleister für PrivatkundInnen, hat in Singapur ein biometrisches Bezahlverfahren für Kreditkarten-Inhabende eingeführt. Mit dem Angebot »Pay By Touch« können BesitzerInnen einer »Clear Platinum Card« Rechnungen in teilnehmenden Geschäften und Bars mit einem digitalen Fingerabdruck quittieren. Das System stammt vom gleichnamigen kalifornischen Unternehmen Pay By Touch, das eigenen Angaben zufolge ca. 3,3 Mio. registrierte KundInnen hat. Mit der »Clear Plantinum Card« adressiert die Citibank Singapur insbesondere jüngere Menschen im Alter von 25 bis 34 Jahre. In ausgewählten In-Läden erhalten sie bei Bezahlung mit der Karte oder dem Fingerabdruck häufig Preisnachlässe. Die für die Teilnahme nötige Hinterlegung der Fingerabdruck-Templates kann an mehreren Orten in Singapur erledigt werden. Beim Enrollment wird auch eine siebenstellige Nummer festgelegt, die bei jedem Bezahlvorgang angegeben werden muss (www.heise.de 21.11.2006).

Malaysia

Kfz-Neuzulassung nur noch mit RFID-Kennung

Die Verkehrsbehörden von Malaysia wollen Neufahrzeuge künftig nur noch mit Nummernschildern zulassen, die eine RFID-Kennung tragen. Die sog. E-Plates lassen sich über stationäre oder mobile Scanner über Entfernungen von bis zu 100 Metern auslesen. Die in die Kennzeichen integrierten Long-Range-Funkchips enthalten Informationen über den Halter sowie Fahrzeugdaten. Die E-Plates sind mit versiegelten Funkchips versehen, die von autorisierten Mechanikern am Fahrzeug verplombt werden. Die integrierten Batterien haben eine Lebensdauer von rund 10 Jahren. Als Ziel der Aktion wird die Eindämmung von Fahrzeugdiebstählen angegeben. Gemäß dem Road Transport Department (RTD) wechseln in Malaysia täglich rund 30 vorrangig hochpreisige Autos widerrechtlich den Besitzer. Auch Großbritannien testet Funknummernschilder mit Long-Range-RFID-Systemen. Dort will man damit z.B. Mautprellern, die vor der Einfahrt in London gefälschte Kennzeichen an ihre Fahrzeuge montieren, leichter auf die Schliche kommen (Omnicard Newsletter Januar 2007).

Südkorea

»Intelligenter« Roboter mit Schusswaffe

Die südkoreanische Regierung plant, ab 2007 an der Grenze zu Nordkorea hunderte von stationären Robotersystemen zur Grenzüberwachung einzusetzen, die autonom entscheiden, ob sie – nachdem sie eine Warnung abgegeben haben, gezielte Schüsse abfeuern. Die Roboter, die September 2006 vom stellv. Minister für Wirtschaft, Industrie und Energie Lee Jae-Hoon vorgestellt wurden, können auch mit einem Joystick und einem Touchscreen-Monitor ferngesteuert werden. Sie sollen danach auch auf dem Markt zur Bewachung von militärischen Einrichtungen wie Flughäfen, Pipelines oder Staudämmen angeboten werden. Die Kosten eines Exemplars werden mit ca. 200.000 Dollar angegeben.

Der Roboter, dessen Kopf sich mit der jeweiligen Waffe und den Sensoren um 180 Grund drehen kann, lässt sich mit einem leichten Maschinengewehr ausstatten oder mit einem Gewehr zum Abfeuern von weniger tödlichen Gummigeschossen. Er kann auch unbewaffnet eingesetzt werden, um bei verdächtigen Ereignissen Alarm auszulösen. Jae-Hoon pries den Roboter als System an, das beobachten, Ziele verfolgen und schießen sowie mit Mustererkennung Menschen, Tiere, Fahrzeuge oder Bäume auf eine Entfernung von zwei Kilometer bei Tageslicht und mit einer Infrarotkamera Nachts bis zu einem Kilometer unterscheiden und verfolgen kann. Bewegte Objekte können tags über bis zu vier, nachts bis zu zwei Kilometer entfernt erkannt werden. Als Sicherheitsmaßnahme ist ein Stimmerkennungssystem vorgesehen, das bis zu einer Entfernung von 10 Metern Freund oder Feind anhand eines gesprochenen Kennwortes unterscheiden soll (www.heise.de 15.11.2006).

Technik-Nachrichten

Neue Verschlüsselungstechnik bei Glasfaser-Übertragung

US-Forschende von der Princeton-University haben eine Methode entwickelt, Daten abhörsicher über öffentliche Glasfaser-Netze zu übertragen, ohne dabei in klassischer Form zu verschlüsseln: Die Nachricht wird in einen kurzen, starken Lichtimpuls umgewandelt und anschließend in einen langen, aber sehr schwachen optischen Datenstrom gespalten. So kann die Information im »Grundrauschen« der Glasfasernetze versteckt werden. Nur wer weiß, wie die Originalnachricht aufgespalten worden ist und ein entsprechendes optisches Geräte bereit hält, kann die eigentliche Nachricht wieder herstellen. Der Methode wird hohe Sicherheit zugesprochen. Selbst wenn jemand wüsste, dass eine geheime Übertragung stattfindet, mache es die kleinste Wissenslücke über den verwendeten Schlüssel immens schwer bis unmöglich, die richtigen Daten herauszufischen (Computer-Fachwissen 11/2006, 26).

RFID-Tags zum Abreißen

Der kanadische Hersteller Labels Marnlen hat die RFID-Chip-Technik »Clipped Tag« von IBM lizensiert und will sofort mit der Produktion und dem Verlauf der neuen Chips beginnen. Nach eigenen Angaben ist Marnlen die

erste Firma, die das Clipped-Tag-Verfahren lizensiert, womit die VerbraucherIn den Großteil der Antenne eines Funklabels an einer Perforierung abtrennen und damit die Reichweite für die Auslesbarkeit des Chips deutlich verringern kann. Die Basisfunktion der Funketiketten wird dabei aber nicht zerstört. IBM hatte die Technik Anfang 2006 als Vorschlag in die Diskussion um datenschutzgerechte RFID-Chips eingebracht und die Technik zusammen mit Marnlen weiterentwickelt (http://www.marnlen.com; Omnicard-Newsletter November 2006/II).

Intelligentes Sportlerhemd fördert Zuschauerüberblick

SportlerInnenhemden könnten demnächst weit mehr über ihre TrägerIn verraten als nur Namen oder Rückennummer. Für seine Abschlussarbeit in »Design Computing« hat der australische Student Mitchell Page ein intelligentes Basketballtrikot ersonnen: Verschiedene Leuchtstreifen, die über eine Bluetooth-Verbindung aktiviert werden können, liefern dabei Informationen über den Spielverlauf. Streifen auf den Schultern zeigen die Anzahls der Fouls an. Je mehr Streifen an der Seite des Trikots leuchten, umso mehr Körbe hat eine SpielerIn bereits geworfen. Geht die Spielzeit zu Ende, beginnt es auf der Brust der AthletIn zu leuchten, bei den SpielerInnen des führenden Teams strahlen die Rückenstreifen. Page erklärt: »Bei schnellen Spielen wie Basketball ist es schwer, den Überblick zu behalten.« Ob sein TeamAwear-Trikot dies ändert oder Stars womöglich aussehen wie ein Rudel Glühwürmer, muss sich erst noch zeigen. Pages Testspieler jedenfalls waren angetan: »Die Sportler fanden das System leicht verständlich und fühlten sich davon nicht abgelenkt (Der Spiegel 49/2006, 159).

Hirnaktivität steuert Zugangskontrolle

Griechische Forscher haben ein System entwickelt, das die Hirnaktivität auf der Basis von Elektroenzephalografie zur biometrischen Zugangskontrolle nutzt. Das System identifiziert Personen anhand der einzigartigen Muster, die durch elektrische Aktivität des Gehirns entstehen. Die aufgezeichneten Gehirnaktivitäten sollen kaum zu fälschen sein. Der Leiter des Entwicklungsteams vom Center for Research and Technology Hellas, Dimitrios Tzovaras meint daher: »Damit ist das System für Anwendungen im High-Security-Bereich geeignet«. Bei dem System wird einer Person eine Kappe aufgesetzt, die mit Elektroden ausgerüstet ist. Diese misst die Hirnströme und zeichnet dabei ein Elektroenzephalogramm (EEG) auf. Die EEGs werden kabellos an den Rechner weitergeleitet und mit früheren Aufnahmen verglichen. Die Software analysiert die Muster der Hirnströme und erkennt die jeweilige Person. Einige Forschende sehen die Methode jedoch skeptisch: Bei Stress könnte sich das EEG stark verändern, so dass eine Identifikation erschwert wird. Ende 2007 soll mit ausführlichen Praxistests begonnen werden (www.testticker.de 23.01.2007).

Gentechnik-Nachrichten

Niedersachsen

Genetische Familienforschung per Massentest

Hunderte Menschen haben sich Ende Januar 2007 in der Grundschule Förste im Kreis Osterode für ein weltweit einzigartiges Forschungsprojekt der Anthropologin Susanne Hummel der Universität Göttingen eine Speichelprobe nehmen lassen. Die WissenschaftlerInnen wollen durch genetische Untersuchungen herausfinden, ob es heute noch Nachfahren eines bronzezeitlichen Familienverbandes gibt, der vor rund 3.000 Jahren im Südharz lebte. Vor einigen Jahren waren 40 Skelette dieser prähistorischen Südharzbewohner in der Lichtensteinhöhle gefunden worden. Die Höhle gilt seitdem als eine der bedeutendsten urgeschichtlichen Fundstätten in Mitteleuropa. Zähne und Knochen waren so gut erhalten, dass die Göttinger ExpertInnen nicht nur das Erbgut der Individuen entschlüsseln, sondern auch die Verwandtschaftsbeziehungen über drei Generationen nachvollziehen konnten. Mit dem neuen Forschungsprojekt soll geklärt werden, ob die damaligen Bewohner des Südharzes die Urahnen der heutigen sind. Eine solche Verwandtschaft wäre die längste bekannte Stammbaumlinie der Welt.

In einem Aufruf in der Lokalpresse wurden die BewohnerInnen der Südharzer Ortschaften Dorste, Förste, Eisdorf, Nienstedt, Marke, Ührde und Schwiegershausen gebeten, sich an dem Projekt zu beteiligen. Die Dörfer liegen in unmittelbarer Nachbarschaft der Lichtensteinhöhle; viele Familien sind seit langem in der Region ansässig. Die Resonanz übertraf alle Erwartungen. Die Leute standen zeitweilig Schlange, um Speichelproben abzugeben. Viele Dorfbewohnenden können ihre Familiengeschichte weit zurückverfolgen. Bernd Zeisberg aus Förste ist begeisterter Ahnenforscher und hat Vorfahren bereits bis zum 17. Jahrhundert ermittelt: »Es wäre doch gut zu wissen, ob es einen Zusammenhang mit den Bronzezeit-Skeletten gibt. Eine Bewohnerin erklärte: »Hier hat man immer von einem Dorf zum anderen geheiratet« (Niemann Frankfurter Rundschau 22.01.2007, 16).

Umfrage

Sprachtest für Kinder

Auf die Frage, ob in Deutschland ein obligatorischer Deutschtest für Vier- bis Fünfjährige eingeführt werden soll, antworteten 87% mit »Ja«, 12% mit »Nein«. Kinder deren Kenntnisse als nicht ausreichend angesehen werden, sollen zu Sprachkursen verpflichtet werden (Der Spiegel 46/2006, 22; vgl. S. 24).

Rechtsprechung

EuG

Europäische Terrorliste verletzt Grund- und Verfahrensrechte

Das Europäische Gericht 1. Instanz (EuG) in Luxemburg hat in einem Urteil vom 12.12.2006 nach vierjähriger Verfahrensdauer aus grundsätzlichen Erwägungen die Aufnahme einer Mudschaheddin-Gruppe in die vom Europäischen Rat aufgestellte Liste der Personen und Organisationen für nichtig erklärt, gegen die wegen des Verdachts der Unterstützung des Terrorismus umfassende Finanzsanktionen verhängt werden (Az. T-228/02). Das bisherige Verfahren, wonach z.B. Gelder von Verdächtigten eingefroren werden dürfen, verletze deren Grund- und Verfahrensrechte. Die Richter verlangten, dass die Betroffenen eine Begründung erhalten und erfahren, welches Land auf Grund welcher Unterlagen die Aufnahme auf die Liste verlangt habe. Nur dann sei es ihnen möglich, sich wirksam zu wehren. Jeder Betroffene habe das Recht, vor Gericht gegen Rechtsverletzungen vorzugehen und sich per Klage zur Wehr zu setzen (SZ 13.12.2006, 8; vgl. DANA 2/2006, 85 f.).

BVerfG

Seelsorgergeheimnis gilt nicht unbegrenzt

Das Bundesverfassungsgericht (BVerfG) hat mit Beschluss vom 29.01.2007 die Verfassungsbeschwerde eines – nicht zum Priester geweihten – katholischen Gemeindereferenten zurückgewiesen, der in einem beim Oberlandesgericht (OLG) Düsseldorf anhängigen Strafverfahren als Zeuge vernommen werden sollte (Az. 2 BvR 26/07). In dem Strafverfahren geht es um Versicherungsbetrug zu Gunsten der Finanzierung des Terrornetzwerkes Al Qaida. Der hauptamtlich als Seelsorger Tätige hatte in seiner Funktion Gespräche mit einem Angeklagten geführt. Er weigerte sich unter Berufung auf sein Seelsorgergeheimnis die Frage zu beantworten, ob er für den Angeklagten im Internet Adressen von Versicherungen recherchiert habe. Das BVerfG hat es offen gelassen, ob das Zeugnisverweigerungsrecht für Geistliche nach der Strafprozessordnung auch für Seelsorger gilt, die keine Priesterweihe erhalten haben. Jedenfalls könne sich ein hauptamtlich von der Kirche Beauftragter auf dieses Verweigerungsrecht berufen. Doch es sei verfassungsrechtlich nicht zu beanstanden, dass die Fachgerichte den Austausch über Recherchen im Internet objektiv nicht zum Seelsorgergeheimnis gezählt haben.

Ein Zeugnisverweigerungsrecht lasse sich auch nicht unmittelbar aus der Verfassung ableiten. Die an den Beschwerdeführer gestellten Fragen seien nicht dem Kernbereich privater Lebensgestaltung zuzurechnen, in den der Staat nicht eingreifen dürfe. Die in Frage stehende Aussage ziele auch nicht auf ein seelsorgerisches Gespräch, sondern auf Recherchen, die der Beschwerdeführer nur außerhalb eines solchen Gesprächs wahrgenommen haben kann. Zwar könne die Preisgabe des Wissens über die dem Gefangenen erwiesene Gefälligkeit das bestehende Vertrauensverhältnis beeinträchtigen und auch die Wahrnehmung der seelsorgerischen Aufgaben erschweren. Doch würden hier die Belange der Strafrechtspflege überwiegen. Es sei eher fern liegend, dass sich ein Gefangener auf die vertrauliche Behandlung einer Bitte an den Seelsorger verlassen kann, die ersichtlich nicht den seelsorgerischen Bereich betrifft, sondern darauf abzielt, Beweisgegenstände zu verfälschen und für den Seelsorger sogar die Gefahr eigener Strafbarkeit begründet. Es bestehe daher eine Zeugenpflicht mit der Folge der Möglichkeit, bis zu 6 Monate Beugehaft zu erwirken.

Nach dem Urteil machte der Seelsorger vor dem OLG Angaben: »Ich stehe nicht über dem Recht; ich muss mich dem Recht beugen.« Es gehöre zur Alltagsarbeit eines Gefängnisseelsorgers für Gefangene auf deren Wunsch Kontakte nach außen herzustellen oder Adressen für deren Briefverkehr zu vermitteln. Er habe bei seinen Internet-Recherchen für den Gefangenen an eine mögliche Strafvereitelung »nie gedacht« (Nitschmann SZ 01.02.2007, 8; PE BVerfG 9/2007 v. 29.01.2007; Kerscher SZ 30.01.2007, 5).

BVerfG

Vaterschaftsklagen werden erleichtert, heimliche Gentests bleiben verboten

Das Bundesverfassungsgericht hat mit Urteil vom 13.02.2007 den Bundestag aufgefordert, bis zum 31.03.2008 das Verfahren zur Feststellung der Vaterschaft neu zu regeln, so dass Männer künftig bei Gericht klären lassen können, ob sie tatsächlich Vater eines Kindes sind. Heimliche Vaterschaftstests sollen jedoch auch künftig nicht als Beweismittel vor Gericht zugelassen werden (Az. 1 BvR 421/05). Diese Tests verletzen das Recht des Kindes auf informationelle Selbstbestimmung. Das Gericht verwies aber darauf, dass zum allgemeinen Persönlichkeitsrecht eines Mannes gehört, ermitteln zu können, ob er tatsächlich Vater eines ihm rechtlich zugeordneten Kindes sei. Bisher habe der Gesetzgeber es »unter Verletzung dieses Grundrechtsschutzes« unterlassen, dafür einen angemessenen Verfahrensweg zu schaffen. Dieser Zustand müsse abgestellt werden.

Das Gericht verwarf mit seiner Entscheidung die Verfassungsbeschwerde eines Mannes, der seine Klage zur Anfechtung der Vaterschaft auf ein heimlich eingeholtes DNS-Gutachten gestützt hatte und damit gescheitert war. Der heimliche Test hatte ergeben, dass er nicht der biologische Vater seines rechtlichen Kindes ist. Die Gerichte erkannten den Beweis aber nicht an, weil die Zustimmung der sorgeberechtigten Mutter zum Test fehlte. Der Mann muss daher weiter vollen Unterhalt bezahlen.

Obwohl der Kläger in seinem Verfahren unterlag, zeigte er sich mit dem Urteil zufrieden: Er habe erreicht, dass das Verfahren für Väter in Zukunft einfacher werde. Bundesjustizministerin

Brigitte Zypries (SPD) begrüßte das Urteil ebenso. Ihr Haus arbeite bereits seit 1 ½ Jahren an einer entsprechenden Neuregelung und diese liege »quasi in der Schublade«. Feststellungen und Anfechtung der Vaterschaft sollen künftig in zwei getrennten Verfahren geregelt werden. So könnten Männer ihre biologische Vaterschaft klären, ohne ihre rechtliche Vaterschaft aufgeben zu müssen. Mit der bisherigen Anfechtungsklage verliert ein Mann im Erfolgsfall zwangsläufig auch seinen Status als rechtlicher Vater, was weitreichende Folgen für das Umgangs-, Sorge- und Unterhaltsrecht hat. Auch beim neuen reinen Feststellungsverfahren soll gewährleistet sein, dass Männer nicht ohne jeden Anhaltspunkt ihre Vaterschaft überprüfen lassen.

Zypries begrüßte auch die Entscheidung des BVerfG zu heimlichen Tests. Zwei Jahre zuvor hatte ihre Ankündigung, in einem Genanalysegesetz für derartige Tests eine strafrechtliche Ahndung von bis zu einem Jahr Haft vorzusehen, eine große Kontroverse ausgelöst. Angesichts dessen warnte die Union die Justizministerin davor, die heimlichen Tests jetzt zu kriminalisieren. Könne der Mann, so der rechtspolitische Sprecher der CDU/CSU-Fraktion Jürgen Gehb, seinen Verdacht nur vor Gericht offenbaren und erweise sich dieser als falsch, sei die Partnerschaft ruiniert. Bei 80% der heimlichen Gentests stellt sich offensichtlich heraus, dass der Mann doch der Vater ist (Prantl SZ 13.02.2007, 5; Roßmann, Kerscher, Charisius, Prantl SZ 14.02.2007, 1, 2, 4; Hipp, Der Spiegel 7/2007, 50, 53; Der Spiegel 8/2007, 19).

BGH

Verdeckte Online-Durchsuchung unzulässig

Die heimliche Durchsuchung der im Computer eines Beschuldigten gespeicherten Dateien mit Hilfe eines Trojaners, also eines Programms, das ohne Wissen des Betroffenen aufgespielt wurde, ist nach einem Beschluss des Bundesgerichtshofes vom 31.01.2007 gemäß den Regelungen der Strafprozessordnung (StPO) unzulässig. Für eine solche verdeckte Online-Durchsuchung fehlt es an der für einen solchen Eingriff erforderlichen Ermächtigungsgrundlage. Der 3. Strafsenat des BGH hat auf die Beschwerde der Generalbundesanwältin gegen den Beschluss des BGH-Ermittlungsrichters Ulrich Hebenstreit vom 25.11.2006 entschieden, der die verdeckte Online-Durchsuchung auch für unzulässig erklärt hatte. Es ging um ein Staatsschutzverfahren gegen einen mutmaßlichen Islamisten. Zuvor hatte ein anderer BGH-Ermittlungsrichter im Februar 2006 eine solche Maßnahme zugelassen.

Gemäß dem Beschluss ist die verdeckte Online-Durchsuchung nicht durch § 102 StPO gedeckt, die die Durchsuchung beim Verdächtigen regelt, weil es sich hierbei um eine offen durchzuführende Ermittlungsmaßnahme handelt. Dies ergibt sich aus Regelungen zu Gunsten des Beschuldigten, etwa dem Anwesenheitsrecht (§ 106 Abs. 1 S. 1 StPO) oder der Zuziehung von Zeugen (§§ 105 Abs. 2, 106 Abs. 1 S. 2 StPO), deren Befolgung als zwingendes Recht nicht zur Disposition der Ermittlungsorgane steht. Dies ergibt sich auch aus einem Vergleich mit Ermittlungsmaßnahmen, die wie die Telekommunikationsüberwachung (§§ 100a, b StPO) oder die Wohnraumüberwachung (§§ 100c, d StPO) ohne Wissen des Betroffenen durchgeführt werden können, für die aber deutlich höhere formelle und materielle Anforderungen an die Anordnung und Durchführung bestehen. Auch andere Befugnisnormen der StPO gestatten die verdeckte Online-Durchsuchung nicht (B. v. 31.01.2007, Az. StB 18/06; zuvor Entscheidung des BGH-Ermittlungsrichters vom 25.11.2006, Az. 1 BGs 184/06, PE BGH 05.02.2007; www.spiegel.de 05.02.2007; vgl. S. 21ff., 26f.).

BGH

Presse hat Recht auf Namensnennung

Wer durch berufliche Tätigkeit ins Blickfeld der Öffentlichkeit gerät, muss bei der Berichterstattung in den Medien grds. die Nennung seines Namens hinnehmen. Die Richter des VI. Zivilsenates des Bundesgerichtshofes (BGH) hoben ein Urteil des Berliner Kammergerichtes auf, das der Nachrichtenagentur dpa untersagte, den Namen des früheren Geschäftsführers einer Klinik zu benennen, dessen Vertrauensverhältnis zum Großteil der Belegschaft nachhaltig gestört gewesen sein soll. Der BGH meinte, Namensnennungen in Berichten über die berufliche Sphäre müssten möglich sein, wenn die Berichterstattung keine schwerwiegenden Auswirkungen auf das Persönlichkeitsrecht habe. Zuvor gab es einige Entscheidungen von Pressekammern, die unter Hinweis auf die Privatsphäre der Betroffenen eine solche Berichterstattung untersagt hatten. Der BGH hob hervor, dass bei der Abwägung zwischen der im Grundgesetz verankerten meinungs- und wertbildenden Funktion der Medien und dem Persönlichkeitsschutz der Anonymitätsschutz des Betroffenen umso mehr zurücktreten müsse, je mehr ein besonderes öffentliches Informationsinteresse bestehe. Im Berliner Fall hatte sich nach dem Gericht ein Akteur des Wirtschaftslebens »in erheblichem Umfang der Kritik an seinen Leistungen« ausgesetzt. Dazu gehöre auch die Erwähnung seines Namens. Es sei nur dann nicht erlaubt, wenn der Betroffene durch die Berichterstattung stigmatisiert werde oder eine »soziale Ausgrenzung oder Prangerwirkung« zu befürchten habe (SZ 01.02.2007, 19).

BVerwG

Verfassungsschutz muss Quellen nennen

Im Verfahren des Bundestagsabgeordneten Bodo Ramelow von der Linkspartei gegen das Bundesamt für Verfassungsschutz (BfV) wegen der erfolgenden geheimdienstlichen Beobachtung hat das Bundesverwaltungsgericht (BVerwG) das Bundesministerium des Innern (BMI) aufgefordert, alle BfV-Akten über den Abgeordneten vorzulegen. BMI und BfV hatten dies unter Hinweis darauf abgelehnt, dass dadurch Quellen bekannt würden. Das BVerwG will aber vor seiner Entscheidung auch die mit Sperrvermerk versehenen Aktenbestandteile sehen (Der Spiegel 6/2007, 18).

VGH Baden-Württemberg

Milli Görus gewinnt gegen Verfassungsschutz wegen Tatsachenbehauptung

Nach einem Urteil des Verwaltungsgerichtshofes Baden-Württemberg (VGH) vom 24.11.2006 hat das Land Baden-Württemberg nicht belegen können, dass bestimmte Passagen in dessen Ver-

fassungsschutzbericht 2001 richtig sind und wurde deshalb verpflichtet, diese Passagen über die islamische Gemeinschaft Milli Görüs unkenntlich zu machen. Es geht um die Behauptung, bei einer Milli-Görüs-Veranstaltung sei skandiert worden: »Hoca, wenn Du sagst, wir sollen kämpfen, dann kämpfen wir. Wenn Du sagst, wir sollen töten, dann töten wir!« Die zitierten Aussagen sollen bei Veranstaltungen in Ulm und in Neu-Ulm gefallen sein. Aus Gründen der Geheimhaltung weigerte sich der bayerische Verfassungsschutz, seine Akten vorzulegen, die baden-württembergische Behörde erlaubte nicht die Vernehmung von V-Leute. Dennoch meinte der baden-württembergische Innenminister Heribert Rech, der Verfassungsschutz werde Milli Görus weiter beobachten, »weil wir bei dieser Organisation weiterhin verfassungsfeindliche Bestrebungen erkennen« (SZ 25./26.11.2006, 6).

VG Arnsberg

Auskünfte an Presse sind unentgeltlich

Behörden dürfen von Journalisten keine Gebühren für Presseauskünfte verlangen. In einem Urteil gegen die Stadt Meschede gab das Verwaltungsgericht (VG) Arnsberg einer Klage des Bundes der Steuerzahler statt, der sich gegen eine Gebühr der Stadt für Auskünfte zur jährlichen Umfrage für die Steuerzahlerzeitschrift zu kommunalen Gebühren wandte. Nach Auffassung der Richter stellt die Gebührenerhebung eine rechtswidrige Beschränkung des presserechtlichen Informationsanspruchs dar (SZ 05.-07.01.2007, 21).

OLG Düsseldorf

Datenübermittlung an Schufa nur nach Interessenabwägung

Das in der Praxis weit verbreitete Verfahren, Kundendaten auf Grund einer generellen Einwilligung in den Allgemeinen Geschäftsbedingungen (AGB) im Einzelfall und ohne ein konkretes wirksames Einverständnis des Kunden an die Schufa weiterzuleiten, ist nach einem Urteil des Oberlandesgerichtes (OLG) Düsseldorf vom 14.12.2006 rechtswidrig (Az. I-10 U 69/06). Ein Leasinggeber hatte Kundendaten an die Schufa gemeldet, nachdem zwischen den Vertragsparteien nach Kündigung des Leasingvertrages über die Höhe der Restforderung Streit entstanden war. In erster Instanz hatte das Landgericht die Datenübermittlung für rechtmäßig erklärt. Auf die Berufung des Klägers hat der Senat des OLG das Urteil abgeändert und den Leasinggeber verpflichtet, auf eine Löschung der Kundendaten bei der Schufa hinzuwirken.

Die formularmäßige AGB-Einwilligung in die Übermittlung der eigenen Daten an die Schufa sei grds. unwirksam, wenn dies ohne die im Bundesdatenschutzgesetz (BDSG) vorgesehene Interessenabwägung geschehe. Im Rahmen dieser Prüfung sind die schutzwürdigen Belange des Betroffenen einerseits und die berechtigten Interessen des Leasinggebers bzw. der Schufa Holdung AG und der Allgemeinheit an der Kenntniserlangung von Daten zur Zahlungsfähigkeit und -willigkeit andererseits zu berücksichtigen. Im konkreten Fall verwiesen die Formularbedingungen zwar auf die nach dem BDSG gebotene Interessenabwägung; diese sei jedoch gänzlich unterblieben. Diese wäre hier unter den besonderen Umständen des Einzelfalls überdies zugunsten des Leasingnehmers ausgegangen (Heidrich www. heise.de 15.12.06; SZ 15.12.06, 32).

LG Köln

Computereigentümer haftet für Internet-Diffamierungen

Das Landgericht (LG) Köln hat mit Beschluss vom 18.10.2006 entschieden, dass der Eigentümer eines Computers für die darüber im Internet veröffentlichte Diffamierungen haftet (Az. 28 O 364/06). Im Juli 2006 waren unter dem Namen des Beklagten im Forum eines Internetportals, auf dem Anwälte gegen Entgelt Fragen von Rechtssuchenden beantworten, diffamierende Äußerungen gegen einen der dort tätigen Juristen eingestellt. Dieser erwirkte daraufhin eine einstweilige Verfügung, die der Beklagte in der mündlichen Verhandlung anerkannte. In seiner Entscheidung entschied das LG über die Verfahrenskosten, die dem Beklagten auferlegt wurden. Dieser bestritt, der Verfasser der Antworten zu sein. Vielmehr habe sein Sohn seine Abwesenheit genutzt, in diesem und in anderen Foren unter dem Namen des Beklagten zu schreiben und juristische Fragen zu beantworten. Der Sohn habe sich auf Grund des in seinem PC ohne sein Wissen gespeicherten Passwortes Zugang zu dem Internetforum verschaffen können. Die Handlungen seien dem Beklagten nicht bekannt gewesen; er habe sich während der fraglichen Zeit auf einer Bergtour befunden.

Nach Ansicht der Richter ist der Anwalt für die von seinem Sohn veröffentlichten Diffamierungen verantwortlich. Dieser hatte nur deshalb Zugang zu dem Internetforum, weil der Nutzername des Beklagten im System bekannt war und das Passwort bei der Eingabe des Nutzernamens im PC automatisch angezeigt wurde. Daher hafte der Vater nach den Grundsätzen der Störerhaftung. Er habe die Verpflichtung, bereits im Vorfeld einer Rechtsverletzung zumutbare und geeignete Vorkehrungen zu treffen, durch welche derartige Handlungen vermieden werden. Die Speicherung von Nutzername und Passwort stelle sich als willentlicher Beitrag dar, durch den der Beklagte an den von seinem Sohn begangenen Rechtsverletzungen mitgewirkt habe. Er konnte sich auch nicht darauf berufen, dass er keine Anhaltspunkte dafür hatte, dass seine Kinder den Account missbräuchlich verwenden würden. Dieses Risiko hätte sich durch einfachste Sicherheitsvorkehrungen zuverlässig ausschließen lassen. Indem der Verfügungsbeklagte insoweit untätig blieb, habe er billigend in Kauf genommen, dass unter seinem Namen Rechtsverletzungen begangen wurden (Heidrich www.heise.de 15.01.2007).

AG Tiergarten

Keine Anwendung von § 38 Abs. 3 BDSG (Auskunftsverlangen der Aufsichtsbehörde für den nicht-öffentlichen Bereich) gegenüber Anwälten

Aus den Gründen: Der Betroffene … ist als selbständiger Rechtsanwalt tätig. Dem Betroffenen ist mit dem Bußgeldbescheid des Berliner Beauftragten für Datenschutz und Informationsfreiheit vom 19.09.2005… zur Last gelegt worden, in der Zeit von November 2004 bis

August 2005 den Berliner Beauftragten für Datenschutz und Informationsfreiheit nicht offenbart zu haben, wie er in den Besitz zweier Briefe gekommen war, die als Strafverteidiger in dem Verfahren… in die Hauptverhandlung eingeführt hat. … Hintergrund für das auf § 38 Abs. 3 BDSG gestützte Auskunftsverlangen der Behörde war, dass sich ein Zeuge aus dem genannten Strafprozess an sie gewandt und sich über die Verlesung der beiden Briefe, welche er ehemals an seinen Vermieter bzw. dessen Hausverwaltung gerichtet hatte, beschwert hatte. Durch die Verweigerung der verlangten Auskünfte soll sich der Betroffene einer Ordnungswidrigkeit nach § 43 Abs. 1 Nr. 10 BDSG schuldig gemacht haben, wobei der Bußgeldbescheid … offen ließ, ob es sich um einen fahrlässigen oder vorsätzlichen Verstoß gehandelt haben soll. …

Der Betroffene war von dem genannten Tatvorwurf aus rechtlichen Gründen freizusprechen, da für den Betroffenen keine Verpflichtung bestand, der Behörde auf der Grundlage von § 38 Abs. 3 S. 1 BDSG die gewünschten Informationen zu erteilen. Der objektive Tatbestand des § 43 Abs. 1 Nr. 10 BDSG war mithin nicht erfüllt. Der Betroffene hat dem ihm zur Last gelegten Sachverhalt in seinem äußeren Ablauf eingeräumt und sich darüber hinaus dahin eingelassen, dass seine anwaltliche Schweigepflicht, von der er auch von seinem Mandanten nicht entbunden worden sei, ihn hindere, dem Auskunftsverlangen des Datenschutzbeauftragten nachzukommen.

§ 1 Abs. 3 S. 1 BDSG gibt vor, dass das Bundesdatenschutzgesetz nur dann anzuwenden ist, wenn keine bereichsspezifische Sonderregelung vorhanden ist – was deutlich macht, dass der Gesetzgeber datenschutzfreie Bereiche ausschließen wollte. Die Bundesrechtsanwaltsordnung (BRAO) stellt eine bereichsspezifische Sonderregelung im Sinne des § 1 Abs. 3 S. 1 BDSG. Speziell die §§ 43 a Abs. 2, 56 Abs. 1, 73 Abs. 2 Nr. 4, 74, 113 ff. BRAO, die die anwaltliche Schweigepflicht, die Auskunftspflicht des Rechtsanwalts gegenüber dem Vorstand der Rechtsanwaltskammer, die Aufsichtspflicht des Vorstandes der Rechtsanwaltskammer, das Rügerecht des Vorstands der Rechtsanwaltskammer und die anwaltsgerichtliche Ahndung von Pflichtverletzungen eines Rechtsanwalts festschreiben, machen die Bundesrechtsanwaltsordnung zu einer bereichsspezifischen Sonderregelung.

Auch wenn § 56 Abs. 1 BRAO in der geltenden Fassung im Hinblick auf für einen effektiven Datenschutz erforderliche Auskünfte als zu allgemein gefasst erscheinen, spricht dies nicht gegen den Charakter der Norm als bereichspezifische Regelung, sondern begründet lediglich ihren Ergänzungsbedarf. Gleiches gilt für den Umstand, dass die sog. anlassfreie datenschutzrechtliche Prüfung gegenwärtig vom Vorstand der Rechtsanwaltskammer wohl nur aufgrund seiner allgemeinen Berechtigung zur umfassenden Berufsaufsicht vorgenommen werden könnte.

Angesichts dieser Weitmaschigkeit und Lückenhaftigkeit der BRAO erscheint auch eine Parallelgeltung von BRAO und § 38 BDSG nicht abwegig. Da der Gesetzgeber in § 38 Abs. 7 BDSG nur für die Gewerbeordnung eine solche Parallelgeltung angeordnet hat, kann von einem entsprechenden gesetzgeberischen Willen im Hinblick auf die BRAO nicht ausgegangen werden.

Daneben fällt auf, dass § 38 Abs. 3 BDSG nicht auf § 24 Abs. 2 S. 1 Nr. 2 und Abs. 6 BDSG verweist, welcher regelt, dass die Kontrolle des Datenschutzbeauftragten von Bund und Ländern sich bei öffentlichen Stellen auch auf Daten erstreckt, die einem Berufsgeheimnis unterliegen. Es darf unterstellt werden, dass der Gesetzgeber eine entsprechende Verweisung vorgenommen hätte, wenngleich es auch bei nicht öffentlichen Stellen – z. B. Rechtsanwälten – beabsichtigt gewesen wäre.

Die Frage, wie das anwaltliche Berufsrecht und das BDSG im Hinblick auf die Verschwiegenheitsverpflichtung des Anwalts zueinander stehen, tangiert den Kern des Anwaltsberufs und ihre Beantwortung setzt eine Begriffsbestimmung der anwaltlichen Tätigkeit voraus.

Das wesentlichste Merkmal anwaltlicher Tätigkeit ist Interessenvertretung und sie beinhaltet mandatsbezogene Datenverarbeitung. Beides macht einen gesteuerten Informationsumgang erforderlich, der ganz entscheidend durch die Wahrung des Berufsgeheimnisses geprägt wird.

Eine Voraussetzung für die Tätigkeit des Rechtsanwalts ist ein Vertrauensverhältnis zwischen Anwalt und Mandanten. Aus Sicht des Mandanten wird hierfür zumeist die Verschwiegenheitsverpflichtung des Anwalts unabdingbare Voraussetzung sein. Dies schließt eine unmittelbare Einwirkung des Staates und eine staatliche Kontrolle in diesem Kernbereich zwingend aus. Insbesondere Strafverteidiger – auch der Betroffene war im vorliegenden Fall als solcher tätig – könnten ihren Beruf, der auch unter dem Schutz von Art. 12 GG steht, kaum ausüben, wenn sie ihren Mandanten nicht zusichern könnten, dass die Informationen, die sie von ihnen erhalten, der staatlichen Kontrolle – auch durch die Hintertür des BDSG – entzogen sind. An dieser Grundsituation vermag der Umstand auch nichts zu ändern, dass der Datenschutzbeauftragte verpflichtet ist, mit den auf der Grundlage eines Auskunftsverlangen nach § 38 Abs. 3 BDSG gewonnenen Informationen verantwortlich umzugehen und diese nicht oder nur in dem Umfange weiterzugeben, wie es der gesetzlich formulierte Auftrag der Behörde erforderlich macht. Bei einer Offenbarungspflicht des Anwaltes würden Anwalt und Mandant die Steuerung und Kontrolle über den weiteren Informationsumfang verlieren. Allein das Wissen des Mandanten hierüber wird in vielen Fällen der Begründung eines Vertrauensverhältnisses zu dem Rechtsanwalt entgegenstehen.

Auf diesem Hintergrund muss dem Rechtsanwalt die Möglichkeit gegeben sein, einem Auskunftsverlangen der Behörde des Datenschutzbeauftragten unter Hinweis auf die anwaltliche Schweigepflicht entgegenzutreten und von § 38 Abs. 3 S. 2 BDSG Gebrauch zu machen, der dem Auskunftspflichtigen gestattet, die Auskunft auf solche Fragen zu verweigern, deren Beantwortung für ihn die Gefahr der Strafverfolgung begründet – etwa nach § 203 StGB, der die Verletzung von Privatgeheimnissen ahndet. (AG Tiergarten, Urteil vom 05.10.2006, GeschZ.: 317 OWi 3235/05.)

AG Frankfurt am Main

Anrufe zu Marktforschungszwecken – ohne Einwilligung zulässig

Das Amtsgericht (AG) Frankfurt am Main hat am 08.01.2007 entschieden, dass Marktforschungsunternehmen BürgerInnen ohne deren vorherige Einwilligung zu Hause anrufen dürfen, da eine repräsentative Forschung nur durch Telefonanrufe möglich sei. AnschlussinhaberInnen würden bei diesen Erstanrufen nur gering belästigt. Die Erhebung von Telefonnummern zur anschließenden Kontaktaufnahme sei nach § 28 Abs. 1 Nr. 2 Bundesdatenschutzgesetz (BDSG) zulässig, da ein berechtigtes Interesse an der Marktfor-

schung bestehe und die Belange der Betroffenen nicht überwiegten. Für einen repräsentativen Querschnitt der gesamten Bevölkerung reiche es nicht aus, PassantInnen in Fußgängerzonen zu befragen oder Briefe zu verschicken, ob sie mit entsprechenden Anrufen einverstanden sind. Zudem könne durch den zersplitterten Telekommunikationsmarkt mit unterschiedlichen Anbietern und Mobilfunknetzen nicht mehr allein anhand des Telefonbuches repräsentativ ausgewählt werden. Für die AnschlussinhaberIn bestehe keine Gefahr, dass sie am Telefon zu einem Vertragsschluss genötigt werde. Das sich anbahnende Gespräch könne sie durch einfaches Auflegen des Hörers beenden.

Das AG meinte weiter, dass die Umfrageunternehmen jene Nummern in sog. Sperrdateien speichern dürfen, von denen bekannt ist, dass deren Inhaberin keine Anrufe zum Zweck der Marktforschung wünschen. § 35 Abs. 2 Nr. 2 BDSG lasse statt einer Löschung von Personendaten ein Sperrung zu, wenn dies im Interesse des Speichernden liegt. Nur mittels einer Speicherung könne sichergestellt werden, dass die dort gespeicherten Rufnummern zukünftig nicht mehr angewählt würden (Az. 32 C 1115/06-22). Das Landgericht (LG) Hamburg hatte kurz zuvor eine Entscheidung des Amtsgerichtes Hamburg vom Oktober 2005 aufgehoben, nach der Anrufe von Marktforschungsunternehmen mit dem Argument der fehlenden Werbeabsicht als noch zulässig erklärt wurden. Das LG meinte dagegen, Anrufe zu Zwecken der Marktforschung seien unzulässige Werbung, wenn »sie von Marktforschungsunternehmen im Auftrag anderer Unternehmen durchgeführt werden und mittelbar der Absatzförderung dienen«. Dies gelte insbesondere, »wenn Verbrauchergewohnheiten im Zusammenhang mit Produkten und Dienstleistungen des Auftraggebers« erfragt werden (Kaufmann, www.heise.de 12.01.2007).

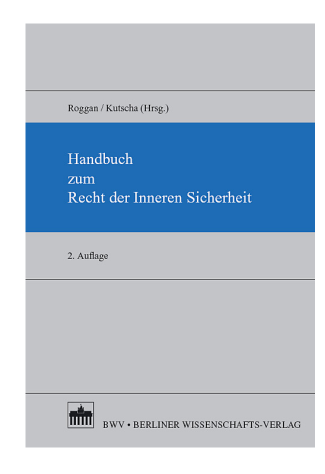
OGH Österreich

Biometrische Stempeluhr ist mitbestimmungspflichtig

Der Oberste Gerichtshof (OGH) Österreichs hat in einem Urteil von Dezember 2006 festgestellt, dass biometrische Zeiterfassungssysteme als Eingriff in die Menschenwürde der Mitbestimmungspflicht unterliegen. Der Betriebsrat eines Krankenhauses wollte per einstweilige Verfügung den Einbau eines Fingerscan-Systems zur Erfassung der Anwesenheitszeiten stoppen und war damit in allen Instanzen erfolgreich. Er hatte zuvor von der Geschäftsführung erfolglos eine Betriebsvereinbarung verlangt. Der OGH erklärte in seinem Urteil, dass durch »übliche« Zeiterfassungssysteme wie Stechuhren oder Magnetkarten die Menschenwürde nicht berührt sei, sofern nicht zugleich Arbeits- oder Bewegungsprofile der Mitarbeiter erstellt würden. Anders verhielte es sich bei biometrischen Systemen: »Auf Grund der beträchtlichen Eingriffs- und Kontrollintensität der Abnahme und Verwaltung von Fingerabdrücken und darauf beruhender Templates wird die Menschenwürde der Arbeitnehmer berührt.«

Dies gelte auch, obwohl keine biometrischen Rohdaten, sondern digitale Templates verwendet wurden, die sich nicht auf den Original-Fingerabdruck zurückführen ließen. Jeder Mensch habe »auch während der Zeit, in der er zur Arbeitsleistung in einem Arbeitsverhältnis verpflichtet ist, u.a. das Recht auf Unversehrtheit der Intimsphäre, auf Freiheit vor unbefugter Abbildung und auf Achtung seines Wertes als menschliches Wesen.« Auch wenn der Arbeitgeber grundsätzlich Kontrollrechte habe, könne »auch die Kontrolle rein dienstlichen Verhaltens zustimmungspflichtig sein«. Durch die »einseitige konsenslose Einführung und Anwendung eines Zeiterfassungssystems, das auf einem biometrischen Fingerscanning der Arbeitnehmer beruht«, verletze der Beklagte die Mitwirkungsrechte des Betriebsrates. Die Kontrolleinrichtung sei daher rechtswidrig und unzulässig (Az. ObA 109/06d; www.heise.de).

Buchbesprechungen



Frederik Roggan, Martin Kutscha (Hrsg.)

Handbuch zum Recht der Inneren Sicherheit

Berliner Wissenschafts-Verlag, Berlin, 2. Aufl. 2006, ISBN 3-8305-12332-5

(sh) Frederik Roggan hatte im Jahre 2003 noch als Alleinautor die erste Auflage des Handbuchs bestritten, das sich nun als Sammelband mit einer unter anderem um Bettina Sokol, Mark Alexander Zöller und Heiner Busch deutlich erweiterten Autorenkreises in Mitherausgeberschaft von Martin Kutscha neu präsentiert. Von seiner inhaltlichen Ausrichtung und Gliederung schließt es an das zuletzt im Jahre 2001 in dritter Auflage erneuerte Handbuch des Polizeirechts von Hans Lisken und Erhard Denninger an, ohne dessen enzyklopädischen Anspruch zu verfolgen. Vielmehr greifen die Autoren gezielt die wesentlichen neuen Entwicklungen im Recht der Inneren Sicherheit als Polizei- und Strafverfahrensrecht und Recht der Nachrichtendienste auf.

Die inhaltliche Zielrichtung macht das Grundsatzkapitel über Innere Sicherheit und Verfassung (Martin Kutscha) deutlich, dass den verfassungsrechtlichen Rahmen staatlich produzierter Sicherheit in einem freiheitlich verfassten Gemeinwesen absteckt. Die folgenden Einzelbetrachtungen widmen sich insbesondere den in den letzten Jahren neu geschaffenen oder aufgrund verfassungsrechtlicher Entwicklungen neu konturierten Überwa-

chungseingriffen wie etwa dem großen Lauschangriff, der Telekommunikationsüberwachung, der Videoüberwachung, der automatisierten Kennzeichenerfassung und Schleierfahndung und auch – wenn auch in noch recht überschaubaren Umfang – dem Einsatz neuer High-Tech-Methoden wie Internetüberwachung, RFID-Technologie und GPS. Der Band wendet sich danach den Verschränkungen der verschiedenen Sicherheitsbehörden und ihrer Aufgabenfelder zu, indem er die Verpolizeilichung der Geheimdienste und die Informationszusammenarbeit von Polizei, Strafverfolgungsbehörden im nationalen und europäischen Maßstab beleuchtet. Dies leisten die Autoren in der von ihnen gewohnten juristischen Qualität und unter ständiger Berücksichtigung der aktuellen (Verfassungs-)Rechtsprechung.

Damit ist ein kompaktes Sammelwerk rechtswissenschaftlicher Betrachtungen auf hohem Niveau entstanden, das sich an der Gesetzgebungs- und Rechtsprechungspraxis orientiert. Unvermeidbare Redundanzen sieht man Herausgebern und AutorInnen dabei gerne nach. Ein für den Leserkreis der Datenschutznachrichten naturgemäß zentrales Thema aber wird in dem Handbuch leider weiterhin nicht systematisch dargestellt: die Rechte und Interventionsmöglichkeiten der Betroffenen.

Den Weg zurück in die Ebene der politischen Betrachtung weist Christian Bomarius in seinem Nachwort, wenn er den weiterhin andauernden Streit um die Bedeutung der Freiheitsrechte in Zeiten mannigfaltiger Bedrohungen der »Inneren Sicherheit« ironisch kommentiert: »Das Grundgesetz war offensichtlich eine Erfindung der 68er. Wie fast alles andere, was diese Generation an Einsichten, Forderungen und Reformen in die Welt gesetzt hat, handelt es sich auch bei der deutschen Verfassung um eine groteske Übertreibung, die ins Fanatische Verschossene Vorstellung von der Welt als gutem Willen, der jeder von der Vernunft geforderten Beschränkung, jedem Zwang der Realität als einziges Wort entgegenhält: Freiheit.«

Wem es um die Freiheit ernst ist und wer fachliche und juristische Argumente in der Auseinandersetzung um die »Innere Sicherheit« zu schätzen weiß, dem seien die Beiträge in dem Handbuch als Argumentationshilfe warm ans Herz gelegt.



Bergmann, Lutz; Möhrle, Roland; Herb, Armin

Datenschutzrecht

Kommentar zum Bundesdatenschutzgesetz, den Datenschutzgesetzen der Länder und zum Bereichsspezifischen Datenschutz

Richard Boorberg, Stuttgart, Loseblattwerk, etwa 2980 Seiten, einschl. 3 Ordnern, 32. Erg.-Lfg. Stand Oktober 2005, ISBN 3-415-00616-6, Grundwerk 84 €

(hhs) Wer sich vertieft mit dem Datenschutzrecht befasst, kommt an dem vorliegenden Werk nicht vorbei. Es bietet einen zusammenfassenden Überblick über das Datenschutzrecht des Bundes und der Länder, den datenschutzrechtlichen Vorschriften des Sozialgesetzbuches I (Allgemeiner Teil), II (Grundsicherung für Arbeitsuchende), IV (Gemeinsame Vorschriften für die Sozialversicherung), V (Krankenversicherung), VI (Rentenversicherung), VII (Unfallversicherung), VIII (Kinder- u. Jugendhilfe), X (Schutz der Sozialdaten) und XI (Pflegeversicherung), dem Melderecht des Bundes und der Länder, den Text der Datenschutzgesetze der Kirchen sowie den vollständigen und aktuellen Text der EU-Datenschutzrichtlinie.

An praktischen Hilfen werden dem Nutzer eine Kommentierung aller Vorschriften des Bundesdatenschutzgesetzes mit Schaubildern, Übersichten und Mustern für die Praxis zur Verfügung gestellt. Ergänzt wird das Werk durch ein Fundstellenverzeichnis zur Erschließung aller Diagramme, Formulare, Kataloge, Merkblätter, Muster, Schaubilder, Synopsen, Tabellen, Überblicke und Übersichten des Kommentars.

Die vorliegende 32. Ergänzungslieferung (Stand Oktober 2005) umfasst die neue Kommentierung von Normen des Bundesdatenschutzgesetzes, welche vorwiegend aus dem öffentlichen Bereich stammen:

- § 18 BDSG Durchführung des Datenschutzes in der Bundesverwaltung,
- § 19 BDSG Auskunft an den Betroffenen,
- § 19 a BDSG Benachrichtigung,
- § 22 BDSG Wahl des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit,
- § 31 BDSG Besondere Zweckbindung,
- § 33 BDSG Benachrichtigung des Betroffenen,
- § 34 BDSG Auskunft an den Betroffenen,
- § 38 BDSG Aufsichtsbehörde sowie
- § 42 BDSG Datenschutzbeauftragter der Deutschen Welle.

Bei § 38 BDSG sind u.a. in einer Anlage 1 die zuständigen Aufsichtsbehörden für die Privatwirtschaft in den einzelnen Bundesländern aufgeführt.

Alles in allem enthält der vorliegende Kommentar viel an Informationen und auch Antworten zu den vielen Spezialitäten, die bei der Anwendung des BDSG auftauchen können. Mithin gehört das Werk zum Standardwerkzeug eines jeden mit Datenschutzrecht Befassten.

Einhellige Ablehnung der Koalitionspläne zur Vorratsspeicherung von Telekommunikationsdaten

Pressemitteilung von 27 Verbänden vom 22.01.2007

27 Verbände lehnen in einer heute veröffentlichten Gemeinsamen Erklärung einen Gesetzentwurf von Bundesjustizministerin Brigitte Zypries ab, dem zufolge künftig Daten über jede Nutzung von Telefon, Handy, E-Mail und Internet auf Vorrat gesammelt werden sollen (sog. »Vorratsdatenspeicherung«), damit sie Polizei und Staatsanwaltschaften zur Verfügung stehen. Die Verbände bezeichnen es als »inakzeptabel«, dass ohne jeden Verdacht einer Straftat sensible Informationen über die sozialen Beziehungen, die Bewegungen und die individuelle Lebenssituation von über 80 Millionen Bundesbürgerinnen und Bundesbürgern gesammelt werden sollen. Getragen wird die Gemeinsame Erklärung von Bürgerrechts-, Datenschutz- und Menschenrechtsverbänden, von Journalistenorganisationen und Medienverbänden, von der Internetwirtschaft und der Telefonseelsorge, von Anwalts- und Juristenverbänden sowie von der Verbraucherzentrale.

Neben einer verbesserten Strafverfolgung begründet die Bundesregierung die geplante Vorratsdatenspeicherung damit, dass eine EG-Richtlinie vom März 2006 umgesetzt werden müsse. Diesem Argument erteilt der Jurist Patrick Breyer vom Arbeitskreis Vorratsdatenspeicherung eine Absage: »Die Richtlinie zur Vorratsdatenspeicherung ist so offensichtlich rechtswidrig, dass Deutschland zu ihrer Umsetzung nicht verpflichtet ist.« Die Gemeinsame Erklärung von heute erläutert: »Die Richtlinie verstößt gegen die im Europarecht verankerten Grundrechte und ist in vertragsverletzender Weise zustande gekommen.« Seit Juli 2006 ist gegen die Richtlinie bei dem Europäischen Gerichtshof eine Nichtigkeitsklage anhängig. Die Verbände fordern, zumindest den Ausgang dieser Klage abzuwarten, bevor eine »derart weitreichende Registrierung des Verhaltens der Menschen in Deutschland« beschlossen wird.

Den angeblichen Nutzen einer Vorratsdatenspeicherung stellt eine ausführliche Analyse des Arbeitskreis Vorratsdatenspeicherung vom Freitag in Frage. Danach fehlten den Strafverfolgern Kommunikationsdaten nur selten. Aus einer Studie des Bundeskriminalamts ergebe sich, dass eine Vorratsdatenspeicherung die durchschnittliche Aufklärungsquote »von derzeit 55% im besten Fall auf 55,006% erhöhen« könne. Eine Vorratsdatenspeicherung hätte in Irland und anderen Staaten keinen ersichtlichen Einfluss auf die Kriminalitätsrate gehabt. »Somit ist nicht erkennbar, dass eine Vorratsdatenspeicherung die Sicherheit der Bevölkerung stärkt.«

Stattdessen würde die Datenspeicherung »Millionen von Euro kosten, die Privatsphäre Unschuldiger gefährden, vertrauliche Kommunikation beeinträchtigen und den Weg in eine immer weiter reichende Massenansammlung von Informationen über die gesamte Bevölkerung ebnen.« Müsse jeder die Aufzeichnung großer Teile seines Kommunikations-, Bewegungs- und Internetnutzungsverhaltens bedenken, seien »Kommunikationsstörungen und Verhaltensanpassungen« zu erwarten. Deshalb schade die Massendatenspeicherung der »freiheitlichen Gesellschaft insgesamt«, so die Stellungnahme des Arbeitskreises Vorratsdatenspeicherung gegenüber dem Bundesjustizministerium.

Die Gemeinsame Erklärung vom 22.01.2007 im Wortlaut:

»Gemeinsame Erklärung zum Gesetzentwurf über die Vorratsdatenspeicherung

Der Gesetzentwurf zur Neuregelung der Telekommunikationsüberwachung sieht vor, Telekommunikationsunternehmen ab Herbst 2007 zu verpflichten, Daten über die Kommunikation ihrer Kunden auf Vorrat zu speichern. Zur verbesserten Strafverfolgung soll nachvollziehbar werden, wer mit wem in den letzten sechs Monaten per Telefon, Handy oder E-Mail in Verbindung gestanden hat. Bei Handy-Telefonaten und SMS soll auch der jeweilige Standort des Benutzers festgehalten werden. Bis spätestens 2009 soll zudem die Nutzung des Internet nachvollziehbar werden.

Eine derart weitreichende Registrierung des Verhaltens der Menschen in Deutschland halten wir für inakzeptabel. Ohne jeden Verdacht einer Straftat sollen sensible Informationen über die sozialen Beziehungen (einschließlich Geschäftsbeziehungen), die Bewegungen und die individuelle Lebenssituation (z.B. Kontakte mit Ärzten, Rechtsanwälten, Psychologen, Beratungsstellen) von über 80 Millionen Bundesbürgerinnen und Bundesbürgern gesammelt werden. Damit höhlt eine Vorratsdatenspeicherung Anwalts-, Arzt-, Seelsorge-, Beratungs- und andere Berufsgeheimnisse aus und begünstigt Wirtschaftsspionage. Sie untergräbt den Schutz journalistischer Quellen und beschädigt damit die Pressefreiheit im Kern. Die enormen Kosten einer Vorratsdatenspeicherung sind von den Telekommunikationsunternehmen zu tragen. Dies wird Preiserhöhungen nach sich ziehen, zur Einstellung von Angeboten führen und mittelbar auch die Verbraucher belasten.

Untersuchungen zeigen, dass bereits die gegenwärtig verfügbaren Kommunikationsdaten ganz regelmäßig zur effektiven Aufklärung von Straftaten ausreichen. Es ist nicht nachgewiesen, dass eine Vorratsdatenspeicherung besser vor Kriminalität schützen würde. Dagegen würde sie Millionen von Euro kosten, die Privatsphäre Unschuldiger gefährden, vertrauliche Kommunikation beeinträchtigen und den Weg in eine immer weiter reichende Massenansammlung von Informationen über die gesamte Bevölkerung ebnen.

Rechtsexperten erwarten, dass das Bundesverfassungsgericht eine Pflicht zur verdachtslosen Vorratsspeicherung von Kommunikationsdaten für verfassungswidrig erklären wird. Außerdem wird erwartet, dass die EG-Richtlinie zur Vorratsdatenspeicherung vor dem Europäische Gerichtshof keinen Bestand haben wird. Die Richtlinie verstößt gegen die im Europarecht verankerten Grundrechte und ist in vertragsverletzender Weise zustande gekommen. Irland hat bereits Klage gegen die Richtlinie erhoben. Der Ausgang dieser Klage sollte zumindest abgewartet werden.

Als Vertreter der Bürgerinnen und Bürger, der Medien, der freien Berufe und der Wirtschaft lehnen wir das Vorhaben einer Vorratsdatenspeicherung geschlossen ab. Wir appellieren an die Politik, sich grundsätzlich von dem Vorhaben der umfassenden und verdachtsunabhängigen Speicherung von Daten zu distanzieren.«

Unterzeichner:
Arbeitskreis Vorratsdatenspeicherung ▪ Bundesverband Deutscher Zeitungsverleger e.V. (BDZV) ▪ Chaos Computer Club e.V. (CCC ▪ Deutsche Journalistinnen- und Journalisten-Union (dju) in ver.di ▪ Deutsche Liga für Menschenrechte e.V. ▪ Deutsche Vereinigung für Datenschutz (DVD) e.V. ▪ Deutscher Journalisten-Verband (DJV) ▪ Deutscher Presserat ▪ eco Verband der deutschen Internetwirtschaft e.V. ▪ Evangelische Konferenz für Telefonseelsorge und Offene Tür e.V. ▪ Förderverein für eine Freie Informationelle Infrastruktur e.V. (FFII Deutschland) ▪ Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung e.V. (FIfF) ▪ Gesellschaft für Datenschutz und Datensicherung e.V. (GDD) ▪ Gustav Heinemann-Initiative (GHI) ▪ Humanistische Union e.V. ▪ Internationale Liga für Menschenrechte (ILMR) ▪ Komitee für Grundrechte und Demokratie e.V. ▪ Netzwerk Neue Medien e.V. ▪ netzwerk recherche e.V. ▪ Neue Richtervereinigung e.V. (NRV) ▪ no abuse in internet e.V. (naiin) ▪ Organisationsbüro der Strafverteidigervereinigungen ▪ Repubikanischer Anwältinnen- und Anwälteverein e.V. (RAV) ▪ STOP1984 ▪ Verband Deutscher Zeitschriftenverleger (VDZ) ▪ Verbraucherzentrale Bundesverband e.V. (vzbv) ▪ Vereinigung Demokratischer Juristinnen und Juristen e.V. (VDJ) ▪ Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V. (FoeBuD)

Ansprechpartner für Presseanfragen:

- Patrick Breyer, Arbeitskreis Vorratsdatenspeicherung, Tel. 0170/5190598
- Dr. Rolf Gössner, Internationale Liga für Menschenrechte (ILMR) e.V., Tel. 0421/703354
- Bettina Winsemann (Twister), STOP1984, twister@stop1984.com, Tel.: 0208/4374729
- Werner Hülsmann, Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) werner@fiff.de, Tel.: 07531/3659056

Vorratsdatenspeicherung: 10.000 wollen gegen Abbildung ihrer Kommunikation nach Karlsruhe ziehen

Pressemitteilung des Arbeitskreises Vorratsdatenspeicherung vom 06.02.2007

Der Widerstand gegen die von der Bundesregierung geplante sechsmonatige Speicherung aller Telefon-, Handy- und E-Mail-Kontakte geht weiter. Nachdem sich im Januar über 30 Datenschutz-, Bürgerrechts-, Juristen-, Wirtschafts- und Medienverbände gegen die »weitreichende Registrierung des Verhaltens der Menschen in Deutschland« ausgesprochen haben, meldet der Arbeitskreis Vorratsdatenspeicherung heute den zehntausendsten Teilnehmer an der vom Arbeitskreis vorbereiteten Verfassungsbeschwerde. Der Arbeitskreis Vorratsdatenspeicherung ist sich sicher, dass die Gerichte nach der Rasterfahndung und den Online-Durchsuchungen auch die Vorratsdatenspeicherung für unzulässig erklären werden. »Es ist ein offensichtlich unverhältnismäßiger Eingriff in unsere Grundrechte, das Kommunikations- und Bewegungsverhalten der gesamten Bevölkerung zu protokollieren, um die Aufklärungsquote um mikroskopische 0,006% steigern zu können«, begründet der Jurist Patrick Breyer vom Arbeitskreis Vorratsdatenspeicherung.

Seit November 2006 ruft der Arbeitskreis zur Anmeldung für eine Verfassungsbeschwerde gegen die geplante Vorratsdatenspeicherung auf. Über 10.000 Personen haben sich schon gemeldet. 2.500 Teilnehmer haben dem Berliner Rechtsanwalt Meinhard Starostik bereits eine schriftliche Vollmacht zugesandt. Eingereicht wird die Verfassungsbeschwerde, wenn und sobald der Bundestag ein Gesetz zur Einführung der Vorratsdatenspeicherung verabschiedet. Jeder zehnte der Beschwerdeführer/innen ist in einem Vertrauensberuf tätig, davon 19% als Journalisten, 7% als Ärzte, Zahnärzte oder Apotheker sowie 5% als Rechtsanwälte. Auch Geistliche, Heilpraktiker, Krankenpfleger, Psychologen, Sozialarbeiter, Sozialpädagogen und Unternehmensberater wehren sich gegen die geplante Abbildung ihrer vertraulichen Kontakte.

Der zehntausendste Beschwerdeführer, Malte W. aus Hamburg, erhält als Dankeschön für seine Unterstützung ein »Schwarzbuch Datenschutz« und ein »PrivacyDongle« des Datenschutzvereins FoeBuD e.V. Mit dem PrivacyDongle kann Malte trotz Vorratsdatenspeicherung weiterhin anonym im Internet surfen. Dass sich auch Straftäter mit technischen Mitteln leicht der staatlichen Datenanhäufung entziehen können, liegt auf der Hand.

Der Aufruf des Arbeitskreises zur Erhebung einer Massenverfassungsbeschwerde ist in der deutschen Geschichte einmalig.

»Die von der Bundesregierung geplante Totalprotokollierung der Telekommunikation der gesamten Bevölkerung ist ebenfalls einzigartig«, begründet der Politikwissenschaftler Ralf Bendrath vom Arbeitskreis Vorratsdatenspeicherung die Aktion. »Frau Zypries will vorsorglich Informationen über unsere Telefonate, Bewegungen und Internetnutzung sammeln lassen für den Fall, dass wir zu Verbrechern werden. Wir sammeln vorsorglich Beschwerdeführer für den Fall, dass SPD und Union dieses verfassungswidrige Vorhaben tatsächlich umsetzen sollten. Wenn die Koalition unzählige Menschen bespitzeln lassen will, dann werden sich auch unzählige Menschen in Karlsruhe dagegen zur Wehr setzen.«

Ansprechpartner für Presseanfragen:

- Patrick Breyer, Arbeitskreis Vorratsdatenspeicherung, Tel. 0170/5190598
- Ralf Bendrath, Netzwerk Neue Medien e.V., bendrath@zedat.fu-berlin.de, Tel.: 0179/2154614
- padeluun, FoeBuD e.V.; presse@foebud.org, Tel: 0521/175254
- Dr. Rolf Gössner, Internationale Liga für Menschenrechte (ILMR) e.V., Tel. 0421/703354
- Bettina Winsemann (Twister), STOP1984, twister@stop1984.com, Tel.: 0208/4374729

Gegen Bürokratie und Staatswillkür

Piloten wehren sich gegen Terrorverdacht

Pressemitteilung der Pilotenvereinigung www.JAR-Contra.de vom 26.01.2007

»Wir sind Opfer einer unerlaubten Rasterfahndung der Behörden und keine potentielle Terroristen« mit diesen Worten erläutert C.-D.Zink, Sprecher der Pilotenvereinigung JAR-Contra, die Bedenken der Luftsportler, die sich gegen immer mehr Überwachungsmaßnahmen und gegen die Abkehr von der Unschuldsvermutung bis zum Schuldbeweis wenden.

Hintergrund sind die rechtlich fragwürdigen Zuverlässigkeitsüberprüfungen, in denen Luftsportler durch eigenen Antrag und auf ihre Kosten beweisen müssen, dass sie keine Terroristen sind. Auch wenn es mittlerweile viele Gerichtsurteile gegen das Vorgehen der Behörden gibt, werden dennoch immer wieder Anträge auf Zuverlässigkeitsüberprüfung (ZÜP) von den Sportlern mit der Drohung erpresst, dass sie sonst ihre Fluglizenz verlieren würden.

Nachdem der Bundesrat im September 2006 offiziell in einer Begründung verlautbaren lies, dass man Privatpiloten als größtmögliches Terror-Risiko ansieht (Drucksache 520/1/06), stellt JAR-Contra die Frage, welcher Aufschrei durch die Öffentlichkeit ginge, stünde in einer offiziellen Begründung eines Bundesratsbeschlusses ein Satz wie »Nach einhelliger Expertenmeinung stellen die Muslime in Deutschland das größte Terror-Risiko dar...«. Abgesehen, dass diese Aussage genauso falsch ist wie die, die der Bundesrat veröffentlicht hat, macht sie doch deutlich, dass ohne konkreten Anlass eine Bevölkerungsgruppe diskriminiert wird, die noch nie in irgend einer Weise im Zusammenhang mit Terroranschlägen aufgefallen ist.

»Wir sind die Ersten, mit denen man Erfahrungen sammeln will, weil wir eine relativ kleine Gruppe sind«, so Zink, »aber Ziel ist die Totalüberwachung möglichst vieler Bürger. Und wir haben geglaubt, solche Zustände gibt es seit 1989 in Deutschland nicht mehr«.

Rückfragen und weitere Informationen:

- Andreas Alin – Tel: 0 97 23 – 93 25 36 Email: andreas@alin.eu
- Markus Hitter – Tel: 0123 12345 – Email: mah@jump-ing.de
- Jürgen Skucek – Tel: 0033388861406 – Email jurgen@skucek.com
- Eckhard Völlm – Tel: 07042 966043 – Email: ev@arcor.de
- Prof. Konrad Vogeler Tel: 035206 30726 oder 0171 / 639 0233
- Joachim Zweiböhmer – Tel: 060438447 – Email: jozwei@web.de
- Dr.Claus-Dieter Zink – Tel: 07150 – 31637 – Email: c@dzink.de

Privatsphäre muss vor heimlichen Online-Durchsuchungen geschützt bleiben

Verfassungsbeschwerde gegen NRW-Verfassungsschutzgesetz eingelegt

Pressemitteilung der Humanistischen Union e.V. vom 9.2.2007

Der Berliner Rechtsanwalt Dr. Fredrik Roggan hat heute, am 9. Februar 2007, eine Verfassungsbeschwerde gegen das neue Verfassungsschutzgesetz von Nordrhein-Westfalen erhoben. Die Beschwerde richtet sich gegen die in diesem Gesetz erstmals eingeführten »Online-Durchsuchungen« von Computern durch Sicherheitsbehörden. Beschwerdeführer sind eine Journalistin und ein Mitglied der Linkspartei.

Seit dem 20. Dezember 2006 darf der Verfassungsschutz von Nordrhein-Westfalen Computer, die mit dem Internet verbunden sind, heimlich ausspähen. Dabei sollen die auf dem Computer gespeicherten Dateien ohne Kenntnis der Betroffenen durchsucht werden können. Zu dieser Befugnis äußerte Dr. Roggan, der auch stellvertretender Bundesvorsitzender der Bürgerrechtsorganisation HUMANISTISCHE UNION ist: »Mit verdeckten Online-Durchsuchungen kann tief in die Privatsphäre von Personen eingegriffen werden, die – aus welchen Gründen auch immer – in das Visier des Verfassungsschutzes geraten sind. Im Einzelfall hat der Geheimdienst damit Zugriff auf Informationen, die ansonsten nur für die Polizei mit einer Hausdurchsuchung zu erlangen wären. Deshalb kann die Online-Durchsuchung einen Eingriff in das Grundrecht auf Unverletzlichkeit der Wohnung darstellen.«

Schlösse sich das Bundesverfassungsgericht dieser Sichtweise an, so wäre die Verfassungsbeschwerde mit großer Wahrscheinlichkeit erfolgreich, denn die Befugnis im Verfassungsschutzgesetz in NRW enthält nicht einmal einen Richtervorbehalt. Der wäre aber verfassungsrechtlich unabdingbar. Roggan stellt weiter fest: »In jedem Fall ist das Gesetz verfassungswidrig, weil es keine Vorkehrungen zum Schutz der Intimsphäre enthält. Wer in Nordrhein-Westfalen auf seinem Rechner auch tagebuchartige Aufzeichnungen oder Fotos von nahen Angehörigen speichert, kann nicht mehr sicher sein, dass solche höchstpersönlichen Sachverhalte nicht staatlicherseits heimlich ausgespäht werden können.«

Ein weiterer Beschwerdepunkt ist die Befugnis des Verfassungsschutzes zur Teilnahme an Kommunikationseinrich-

tungen des Internets, also beispielsweise Chatrooms. Roggan hierzu: »Hier wird erstmals gesetzlich eine Mitwirkung des Geheimdienstes an Veranstaltungen, die er seinem Auftrag entsprechend eigentlich nur zu beobachten hätte, zugelassen. Dass dies ein Irrweg ist, hat das Bundesverfassungsgericht zuletzt im NPD-Verbotsverfahren herausgestellt.« Das Verbot war daran gescheitert, dass aufgrund der Involvierung von Verfassungsschutzbehörden in die Parteiarbeit nicht ausreichend erkennbar war, ob es sich bei der NPD nicht letztlich um eine »staatliche Veranstaltung« handelte.

Für Rückfragen steht Ihnen Dr. Fredrik Roggan unter Telefon 0174 753 00 79 zur Verfügung.

Humanistische Union e.V., Greifswalder Straße 4, 10405 Berlin, Tel. 030 / 204 502 56, www.humanistische-union.de

Schäubles Daten-Exhibitionismus gefährdet die Sicherheit der Europäer

Pressemitteilung der Bürgerrechtsorganisationen Netzwerk Neue Medien, STOP1984 und FoeBuD vom 12.02.2007

Zum Europäischen Polizeikongress, der diese Woche in Berlin stattfinden wird, erklären die Bürgerrechtsorganisationen Netzwerk Neue Medien, STOP1984 und FoeBuD: Laut Pressemitteilung vom 26.1. will der Bundesinnenminister den USA verstärkten Zugriff auf persönliche Daten von Deutschen gewähren. Diesen Daten-Ausverkauf lehnen wir entschieden ab. Stattdessen müssen sich Deutschland und die EU dafür einsetzen, dass Daten von Europäern in den USA gesetzlich geschützt werden und dass wir vor den amerikanischen Gerichten gegen Missbrauch und Fehlentscheidungen der amerikanischen Sicherheitsbehörden und Geheimdienste klagen können.

Wenn Bundesinnenminister Schäuble ein Abkommen über einen verstärkten Austausch personenbezogener Daten mit den USA anstrebt, dann ignoriert er, dass die USA alle ihnen übermittelten Informationen dazu nutzen, um

- Europäer als vermeintliches Sicherheitsrisiko einzustufen,
- Europäer bei der Einreise festzuhalten und zu vernehmen oder ihnen die Einreise gänzlich zu verweigern,
- Europäer im Ausland aufzugreifen und sie in Geheimgefängnisse wie Guantanamo zu verbringen, wo sie zeitlich unbeschränkt ohne Anspruch auf ein gerichtliches Verfahren festgehalten und unter Anwendung von Foltermethoden verhört werden,
- an Europäern die Todesstrafe zu vollstrecken,
- die elektronische Kommunikation (Telefon, E-Mail, Internet) von Europäern mithilfe des weltweiten Abhörnetzwerks ECHELON dauerhaft zu überwachen und zu analysieren,
- Geldüberweisungen von Europäern zu überwachen (SWIFT) und Bankkonten von Europäern einzufrieren,
- die erlangten Informationen quasi lebenslänglich auf Vorrat abzuspeichern, um sie den Betroffenen bei Bedarf auch nach 30 oder 50 Jahren noch vorhalten zu können,
- die erlangten Informationen freizügig an andere Behörden und Geheimdienste weiterzustreuen, innerhalb der USA wie auch an ausländische Unrechtsstaaten (z.B. Philippinen).

In den USA gibt es keinen gesetzlichen Schutz personenbezogener Daten und keine gerichtliche Kontrolle der Verarbeitung personenbezogener Daten von Europäern. Die Verwendung personenbezogener Daten ist weder sachlich noch zeitlich oder mengenmäßig nennenswert begrenzt. Vorschriften über den Umgang von Geheimdiensten mit den Daten von Nichtamerikanern gibt es nicht oder sie werden geheim gehalten. Die wenigen vorhandenen Schutzgesetze sind auf amerikanische Staatsangehörige beschränkt. Mit dem Argument der nationalen Sicherheit nimmt der Präsident der USA für sich in Anspruch, Entscheidungen frei von jeder Kontrolle treffen zu dürfen.

Der amerikanische Geheimdienst CIA führt eine Liste angeblicher Terrorverdächtiger, in welcher mehr als 190.000 Personen aufgeführt sind. Daneben haben die USA unzählige Menschen auf Flugverbotslisten gesetzt. Zehntausende Einträge waren erwiesenermaßen falsch. Man kann kein Gericht anrufen, um gegen die willkürliche Eintragung auf einer solchen Liste vorzugehen. Sogar der amerikanische Senator Edward Kennedy stand im Jahr 2004 auf einer Flugverbotsliste und hatte große Schwierigkeiten, seinen Namen wieder löschen zu lassen. Die amerikanischen Behörden und Geheimdienste beobachten und infiltrieren friedliche Bürgerrechts-, Umwelt-, Friedens- und Glaubensgruppen (darunter ACLU, Greenpeace und 28 weitere Gruppen und Aktivisten). In den USA kann schon eine kritische Meinungsäußerung (z.B. über die Politik von Präsident Bush, über den Irakkrieg oder über Guantanamo) dazu führen, dass Europäer als »Sicherheitsrisiko« eingestuft werden. Schon wer ein T-Shirt mit kritischer Aufschrift trägt oder regierungskritische Bücher bestellt hat, muss mit drakonischen Maßnahmen rechnen.

Es kann nicht sein, dass wir den USA Daten übermitteln, damit sie uns noch weiteren solchen Nachteilen aussetzen können.

Eine internationale Vergleichsuntersuchung von Privacy International aus dem Jahr 2006 kommt zu dem Ergebnis, dass das Datenschutzniveau der USA etwa dem von Thailand und den Philippinen entspricht. Es gebe in den USA »wenige Sicherungen und eine verbreitete Überwachungspraxis«. In keinem anderen Land sei der gesetzliche Schutz persönlicher Daten und die unabhängige Kontrolle der Datenverarbeitung so gering wie in den USA.

Vor diesem Hintergrund ist es ein Verrat europäischer Interessen, wenn der deutsche Innenminister unsere Daten an Staaten wie die USA weitergeben will. Wir Europäer können durch einen solchen Austausch nur verlieren. Solange die USA die Daten von Europäern nicht gesetzlich schützen und es dort keinen Rechtsschutz für Nichtamerikaner gibt, darf es keine Übermittlung europäischer Daten in die USA geben. Dies verbietet auch die Europäische Menschenrechtskonvention, die uns vor der Übermittlung unserer Daten an unsichere Drittstaaten schützt. Um die USA zur Einführung ausreichender Schutzvorkehrungen zu

bewegen, kommt eine Aufhebung der Visumsbefreiung für US-Amerikaner, der Entzug von Landerechten für amerikanische Fluggesellschaften und ähnliche Mittel in Betracht, welche die USA in vergleichbaren Situationen in der Vergangenheit ihrerseits ohne Bedenken gegen Europäer eingesetzt haben.

Es gibt auch kein berechtigtes Bedürfnis nach einem verstärkten Datenaustausch. Schon heute bestehen Rechtshilfeabkommen zwischen der EU sowie Deutschland und den USA, welche die Zusammenarbeit im Rahmen konkreter Ermittlungsverfahren ermöglichen. Schon diese Abkommen versäumen es, die Sicherheit der betroffenen Europäer zu gewährleisten, weil die USA mit den erhaltenen Daten beliebig verfahren können und die Verwendung der Informationen weder gerichtlich noch von einem unabhängigen Datenschutzbeauftragten kontrolliert wird.

Wie verwahren uns dagegen, dass der Bundesinnenminister unsere Grundrechte weiter ausverkauft. Wir fordern den Bundesinnenminister stattdessen auf, sich im Rahmen der deutschen Ratspräsidentschaft dafür einzusetzen, dass Daten von Europäern in den USA endlich gesetzlich geschützt werden und dass wir vor den amerikanischen Gerichten gegen Missbrauch und Fehler der amerikanischen Sicherheitsbehörden und Geheimdienste vorgehen können. Diese rechtsstaatlichen Mindeststandards für Europäer und andere Nichtamerikaner müssen in den USA allgemein eingeführt werden, auch für Daten, welche die USA selbst erheben. Schließlich dürfen Verträge mit den USA und anderen Staaten, die in unsere Grundrechte eingreifen, nur mit vorheriger parlamentarischer Zustimmung beschlossen werden. Dass dieses demokratische Grundprinzip gegenwärtig nicht gewährleistet ist, muss bei den Menschen auf Unverständnis stoßen und die Politikverdrossenheit der Menschen weiter bestärken.

- Netzwerk Neue Medien e.V. (NNM)
- STOP1984
- Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V. (FoeBuD)

Ansprechpartner für Presseanfragen:

- padeluun, FoeBuD e.V., presse @foebud.org, Tel: 0521/175254
- Bettina Winsemann (Twister), STOP1984, twister@stop1984.com, Tel.: 0208/4374729
- Patrick Breyer, P.Breyer@datenspeicherung.de, Tel. 0170/5190598

Marke »Made in Germany« durch Pläne des Innenministeriums beschädigt

Anbieter-Initiative »IT Security made in Germany« lehnt verdeckte Online-Durchsuchungen ab

Presseerklärung der Anbieter-Initiative IT Security made in Germany (ITSMIG) vom 13.03.2007

Die Pläne des Bundesinnenministeriums, verdeckte Online-Durchsuchungen durchzuführen, stoßen auf massive Kritik aus der IT-Sicherheits-Wirtschaft. Die in der Exportinitiative »IT Security made in Germany (ITSMIG)« zusammengeschlossenen 34 deutschen Anbieter lehnen die Pläne aus dem Innenministerium einhellig ab.

»Schon allein die Diskussion, ob in Deutschland auf Computerfestplatten die Kernbereiche privater Lebensführung vom Staat durchschnüffelt werden dürfen, schadet uns nachhaltig im Ausland«, so Frank Fuchs, Sprecher des Steuerkreises von ITSMIG und CEO von Softpro. »Wir erhalten aus dem Ausland zunehmend Anfragen, weshalb Deutschland nun gleiche Methoden anwenden wolle, wie man sie bisher nur anderen Staaten unterstellt«, so Fuchs weiter.

Übereinstimmend berichten die Mitglieder von ITSMIG, dass bereits das Bekanntwerden der Pläne die deutsche IT-Sicherheitsbranche und die Herkunftsbezeichnung »Made in Germany« diskreditiert sowie deren Vertrauenswürdigkeit unterhöhlt. »Bisher konnten und können deutsche Anbieter zur Absicherung der Informationstechnologie im Ausland auch deshalb punkten, weil man Produkten und Dienstleistungen aus Deutschland mehr vertraut als aus anderen Herkunftsländern«, so Antonius Sommer, ebenfalls Mitglied im Steuerkreis der Initiative und Geschäftsführer der TÜV Informationstechnik. »Dass der deutsche Staat uns in seiner Überwachungsgier nun einen »Bundestrojaner« unterjubeln will, ist katastrophal.« Konsequenterweise schlagen Fuchs und Sommer den Begriff »Bundestrojaner« als Unwort des Jahres 2007 vor.

Verdeckte Online-Durchsuchungen widersprechen dem Geist der im Juni 1999 von der damaligen Bundesregierung beschlossenen Eckpunkte der deutschen Kryptopolitik. Darin hat die Bundesregierung zum Ausdruck gebracht, dass sie in der Verwendung sicherer Verschlüsselung eine entscheidende Voraussetzung für den Datenschutz der Bürger und für den Schutz von Unternehmensgeheimnissen sieht und Maßnahmen ergreifen wird, um die internationale Wettbewerbsfähigkeit deutscher Hersteller von sicheren Verschlüsselungsprodukten zu stärken.

Das Bundesjustizministerium äußert sich kritisch zu den Plänen des Bundesinnenministeriums. Das Bundesministerium für Wirtschaft und Technologie unterstützt die Exportinitiative der deutschen Anbieter und verweist auf die Befürchtungen der deutschen Hersteller von IT-Sicherheitstechnik. Die Eckpunkte des Kryptobeschlusses von 1999 seien weiterhin Grundlage der Politik der Bundesregierung und insofern wird das heimliche Ausspähen von Computern als problematisch angesehen.

Bislang haben die deutschen Anbieter im internationalen Wettbewerb gute Karten. Noch gilt die deutsche Herkunft Anwendern als Garant, vor undokumentierten Hintertürchen – so genannter »Backdoors« – verschont zu bleiben. Neben der hohen Produktqualität ist dies ein ganz wichtiges Merkmal des Leistungsversprechens der IT-Sicherheitsbranche, verbunden mit der Herkunftsbezeichnung »Made in Germany«.

Die Mitglieder von ITSMIG warnen das Bundesinnenministerium eindrücklich davor, im Ausland das Ansehen deutscher Produkte zu verspielen. Sie haben dabei das Negativbeispiel von Anbietern aus den USA vor Augen: Dort fordern Politiker immer wieder, staatlichen Stellen eine Überwachung durch die Hintertür zu ermöglichen.

Unter Berufung auf den Kampf gegen Terrorismus und das Gemeinwohl sollen die nötigen Zugangsdaten unter Aufsicht von Gerichten für Geheimdienste wie den NSA einsehbar sein. Amerikanischen Anbietern fällt es entsprechend schwer, glaubwürdig zu versichern, dass bei ihren Produkten die US-Behörden nicht mithören. Der Sprecher des ITSMIG-Steuerkreises, Frank Fuchs, appelliert folglich eindringlich an die Politik: »Wir dürfen den guten Ruf von IT-Sicherheitslösungen »Made in Germany« nicht leichtfertig aufs Spiel setzen«.

Über die Initiative IT Security made in Germany: In der Initiative IT Security made in Germany (ITSMIG) befinden sich derzeit 34 führende Firmen der deutschen IT-Sicherheitswirtschaft. Thematisiert wird höherwertige IT-Sicherheit, wie z. B. Biometrische Verfahren, Smartcards, Verschlüsselungstechnologien und Public Key Infrastrukturen. Mitglieder sind Hersteller, Systemanbieter und Sicherheitsdienstleister, die den strengen Aufnahmekriterien gerecht wurden. Das Netzwerk agiert als Brückenbauer zwischen seinen Mitgliedern und ausländischen Kunden und Partnern. Die Initiative wird gefördert und unterstützt vom Bundesministerium für Wirtschaft und Technologie (BMWi) und arbeitet als Public Private Partnership (PPP). Das Management liegt beim ITSMIG Steuerkreis, das Projektbüro beim Fraunhofer-Institut für Sichere Informationstechnologie (SIT).

Ansprechpartner für die Presse:

- Sprecher der Initiative ITSMIG: Frank Fuchs, c/o Softpro GmbH, Wilhelmstraße 34, 71034 Böblingen, Telefon: +497031/6606-0, Fax: +497031/6606-66, Mobil: +49160/4788500, ffu@softpro.de
- Public Relations der Initiative ITSMIG: Oliver Küch, c/o Fraunhofer-Institut für Sichere Informationstechnologie SIT, Rheinstraße 75, 64295 Darmstadt, Telefon: +496151/869-213, Fax: +496151/869-224, oliver.kuech@sit.fraunhofer.de

Freiheit statt Angst – Demo gegen Sicherheits- und Überwachungswahn

Aufruf zur Demo in Frankfurt (Main) am Samstag, den 14. April ab 15 Uhr

Pressemitteilung verschiedener Bürgerrechtsgruppen vom 14.03.2007

Bürgerrechtler rufen zu einer bundesweiten Demonstration gegen die ausufernde Überwachung durch Staat und Wirtschaft auf. Am Samstag, den 14. April 2007 werden besorgte Bürgerinnen und Bürger in Frankfurt am Main unter dem Motto »Freiheit statt Angst« auf die Straße gehen. Treffpunkt ist der Hauptbahnhof um 15 Uhr. Der Protestmarsch durch die Stadt wird mit einer Kundgebung vor der Paulskirche enden.

Der Überwachungswahn greift um sich. Staat und Unternehmen registrieren, überwachen und kontrollieren uns immer vollständiger. Egal, was wir tun, mit wem wir sprechen oder telefonieren, wohin wir uns bewegen oder fahren, mit wem wir befreundet sind, wofür wir uns interessieren, in welchen Gruppen wir engagiert sind – der »große Bruder« Staat und die »kleinen Brüder« aus der Wirtschaft wissen es immer genauer.

Mit der Vorratsspeicherung der Telekommunikation und Online-Durchsuchungen von Computern stehen weiter verschärfte Sicherheits- und Überwachungsbefugnisse auf der politischen Agenda. Dabei bewirkt die zunehmende elektronische Erfassung und Überwachung der gesamten Bevölkerung keinen verbesserten Schutz vor Kriminalität, kostet Millionen von Euro und gefährdet die Privatsphäre Unschuldiger. Wo Angst und Aktionismus regieren, bleiben gezielte und nachhaltige Maßnahmen zur Stärkung der Sicherheit ebenso auf der Strecke wie ein Angehen der wirklichen, alltäglichen Probleme der Menschen (z.B. Arbeitslosigkeit und Armut).

Hinzu kommt: Wer sich ständig überwacht und beobachtet fühlt, kann sich nicht mehr unbefangen und mutig für seine Rechte und eine gerechte Gesellschaft einsetzen. Es entsteht allmählich eine unkritische Konsumgesellschaft von Menschen, die »nichts zu verbergen« haben und dem Staat gegenüber – zur vermeintlichen Gewährleistung totaler Sicherheit – ihre Freiheitsrechte aufgeben. Eine solche Gesellschaft wollen wir nicht!

Um gegen Sicherheitswahn und die ausufernde Überwachung zu protestieren, gehen wir am Samstag, den 14. April 2007 in Frankfurt am Main unter dem Motto »Freiheit statt Angst« auf die Straße. Treffpunkt ist der Hauptbahnhof um 15 Uhr. Der Protestmarsch durch die Stadt wird mit einer Kundgebung vor der Paulskirche enden. In der Paulskirche wurden 1848 die ersten Grundrechte auf deutschem Boden erarbeitet. Heute bedroht die grenzenlose Sicherheitslogik der Politik die historische Errungenschaft der Grundrechte.

Wir rufen alle Bürgerinnen und Bürger auf, an der Demo teilzunehmen. Die Politiker sollen sehen, dass die Bürger für ihre Freiheiten wieder auf die Straße gehen! Auf der Demo-Homepage (http://www.Freiheit-statt-Angst.de) finden sich jeweils die neuesten Infos zur Demo, zu Anreisemöglichkeiten und zu Möglichkeiten, mitzuhelfen.

Unsere Forderungen:

1. Weniger Überwachung, wir fordern:

- keine Totalprotokollierung von Telefon, Handy und Internet (Vorratsdatenspeicherung),
- keine geheime Durchsuchung von Computern,
- Stopp der Videoüberwachung des öffentlichen Raums, keine automatische Gesichtskontrolle,
- Stopp von Biometrie und RFID-Chips in Ausweisen und Pässen,
- keine Aufzeichnung des Flugreiseverkehrs,

- kein automatischer Kfz-Kennzeichenabgleich auf öffentlichen Straßen.

2. Bestehende Überwachungsgesetze auf den Prüfstand stellen:

- Wir fordern eine unabhängige Überprüfung aller seit 1968 beschlossenen Überwachungsgesetze auf ihre Wirksamkeit und schädlichen Nebenwirkungen.

3. Stopp für neue Überwachungsgesetze:

- Nach der inneren Aufrüstung der letzten Jahre fordern wir einen sofortigen Stopp neuer Gesetzesvorhaben auf dem Gebiet der inneren Sicherheit, wenn sie mit weiteren Grundrechtseingriffen verbunden sind.

Unterstützer:
Arbeitskreis Vorratsdatenspeicherung ▪ Chaos Computer Club e.V. ▪ Deutsche Vereinigung für Datenschutz e.V. ▪ Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e.V. ▪ FoeBuD e.V. ▪ Humanistische Union e.V. ▪ Leipziger Kamera e.V. ▪ Netzwerk freies Wissen ▪ Netzwerk Neue Medien e.V. ▪ Piratenpartei Hessen ▪ STOP1984

Ansprechpartner für Presseanfragen:

- padeluun, FoeBuD e.V., presse @foebud.org, Tel: 0521/175254
- Bettina Winsemann (Twister), STOP1984, twister@stop1984.com, Tel.: 0208/4374729
- Patrick Breyer, P.Breyer@datenspeicherung.de, Tel. 0170/5190598
- Ralf Bendrath, Tel. 0179-2154614, bendrath@zedat.fu-berlin.de
- Werner Hülsmann, Tel.: 07531-3659056 oder 0177-2828681, werner @fiff.de

EG-Kommission fürchtet um Richtlinie zur Vorratsdatenspeicherung

Pressemitteilung des Arbeitskreises Vorratsdatenspeicherung vom 25.03.2007

Die EG-Kommission hat den Zugang zu Dokumenten abgelehnt, die die Gültigkeit der Richtlinie zur Vorratsspeicherung von Telekommunikationsdaten betreffen. Bürgerrechtler werten die Entscheidung als Ausdruck einer zunehmenden Nervosität der Brüsseler Behörde in Bezug auf eine laufende Klage gegen die Richtlinie.

Der im März 2006 beschlossenen Richtlinie zufolge soll zur verbesserten Strafverfolgung unter anderem nachvollziehbar werden, wer mit wem in den letzten sechs Monaten per Telefon, Handy oder E-Mail in Verbindung gestanden hat. Zwei Monate nach Beschluss der Richtlinie hat der Europäische Gerichtshof die Fluggastdatenübermittlung in die USA für unzulässig erklärt mit der Begründung, dass die EG für die innere Sicherheit nicht zuständig ist. Unter Berufung auf dieses Urteil hat Irland im Juni 2006 Nichtigkeitsklage gegen die Richtlinie zur Vorratsdatenspeicherung eingereicht. Eine Entscheidung des Gerichtshofs wird für nächstes Jahr erwartet.

Unter Berufung auf Informationsfreiheitsregelungen hat der Arbeitskreis Vorratsdatenspeicherung, ein bundesweiter Zusammenschluss von Bürgerrechtlern, Datenschützern und Internet-Nutzern, von der EG-Kommission die Herausgabe von Dokumenten über die Gerichtsverfahren zur Vorratsdatenspeicherung und zur Fluggastdatenübermittlung verlangt. Die Dokumente sollen die Einschätzung vieler Rechtsexperten untermauern, dass die Richtlinie zur Vorratsdatenspeicherung nichtig ist und deswegen nicht umgesetzt werden darf. Die Kommission hat die Anträge nun mit dem Argument abgelehnt, eine Offenlegung könne dem laufenden Gerichtsverfahren schaden und die »Verteidigungsrechte der Parteien unterminieren«.

»Angesichts des stetig wachsenden öffentlichen Interesses an Vorratsdatenspeicherung und Flugdatenübermittlung ist die Ablehnungsbegründung absurd«, kommentiert Twister (Bettina Winsemann) vom Arbeitskreis Vorratsdatenspeicherung. »Die Kommission bewertet hier die kaum nachvollziehbare 'Geheimhaltung' höher als das öffentliche Interesse und schreibt im gleichen Moment, dass die wesentlichen Argumente bereits veröffentlicht wurden. Wenn dem so ist, ist nicht nachvollziehbar, warum die Dokumente nunmehr nicht freigegeben werden. Die gesamte Argumentation ist für mich nicht überzeugend. Ich vermute, dass die Dokumente nur deshalb nicht freigegeben werden, weil man den Gegnern der geplanten Totalprotokollierung der Telekommunikation nicht noch weitere Argumente liefern will.«

In Deutschland laufen Datenschutzbeauftragte gemeinsam mit Journalisten-, Medien-, Verbraucher- und Wirtschaftsverbänden Sturm gegen die Pläne der Bundesregierung, die Kommunikationsdatenspeicherung noch dieses Jahr umzusetzen. »Eine derart weitreichende Registrierung des Verhaltens der Menschen in Deutschland halten wir für inakzeptabel«, heißt es in einer Gemeinsamen Erklärung vom Januar. Die Verbände verlangen, die Pläne zumindest bis zur Entscheidung des Europäischen Gerichtshofs über die Rechtmäßigkeit der Richtlinie auf Eis zu legen. Diese Woche beraten Koalitionspolitiker in Berlin über den Gesetzentwurf der Bundesjustizministerin zur Einführung der Vorratsdatenspeicherung.

Die Bescheide der EG-Kommission im Wortlaut:
wiki.vorratsdatenspeicherung.de/images/Irland-Bescheid.pdf
wiki.vorratsdatenspeicherung.de/images/EP-Bescheid.pdf

Ansprechpartner für Presseanfragen:

- Bettina Winsemann (Twister), STOP1984, twister@stop1984.com, Tel.: 0208/4374729
- Patrick Breyer, P.Breyer@datenspeicherung.de, Tel. 0170/5190598
- padeluun, FoeBuD e.V., presse @foebud.org, Tel: 0521/175254
- Ralf Bendrath, Tel. 0179-2154614, bendrath@zedat.fu-berlin.de
- Werner Hülsmann, Tel.: 07531-3659056 oder 0177-2828681, werner @fiff.de

Fast 2.000 Menschen demonstrierten in Frankfurt für »Freiheit statt Angst«

Pressemitteilung des FoeBuD e.V. vom 15.04.2007

Ein Riesenerfolg: Fast 2.000 Menschen gingen in Frankfurt unter dem Motto »Freiheit statt Angst« gegen Sicherheits- und Überwachungswahn auf die Straße. Sie folgten einem Aufruf des Arbeitskreises Vorratsdatenspeicherung und vieler weiterer Unterstützergruppen, darunter FoeBuD, Chaos Computer Club und Humanistische Union.

padeluun vom FoeBuD e.V. rief in seiner Ansprache auf dem Platz der Republik dazu auf, nicht für eine Illusion von Sicherheit die Freiheitsrechte aufzugeben, für die unsere Vorfahren unter Einsatz ihres Lebens gekämpft hätten.

Heide Lemhöfer, Vertreterin des Vorstands der Ev. Konferenz für Telefonseelsorge, erinnerte: »Ein Mensch hat das Recht, dass es sein persönliches Geheimnis sein und bleiben darf, wenn er Kontakt zu Seelsorge-Einrichtungen aufnimmt, eben auch wenn das per Telefon oder im Internet geschieht. Es geht nicht um irgendwelche Daten, sondern um Menschen mit Leib und Seele, die frei und geschützt reden können müssen, wenn sie nicht an manchem ersticken wollen.

Patrick Breyer, forderte in seiner Ansprache einen Stopp der Pläne, sämtliche Kommunikationsdaten ohne Anfangsverdacht flächendeckend zu speichern (Vorratsdatenspeicherung).

Am Rande des Protestzugs durch die Stadt wurden die Passanten satirisch zur freiwilligen Abgabe von Speichelproben aufgefordert. Eine im Rollstuhl sitzende lebende Kamera »beobachtete« Passanten und Demonstranten. Mit Rufen wie »Freiheit stirbt mit Sicherheit«, »Stoppt den Überwachungswahn« und »Datensammler sind Verbrecher« unterstützten die Teilnehmerinnen und Teilnehmer die Forderung nach mehr Freiheit statt Sicherheitswahn.

Patrick Breyer vom Arbeitskreis Vorratsdatenspeicherung sagte: »Die wahre Gefahr für unsere Demokratie sind nicht Terroristen in Afghanistan, sondern Grundrechtsterroristen hier in Deutschland!«

Bettina Winsemann (Twister) von STOP1984 wandte sich gegen die Behauptung, Datenschutz sei Täterschutz. Gerade in sensiblen Bereichen wie Gesundheit oder Seelsorge sei Datenschutz nicht Täterschutz, sondern Opferschutz.

padeluun vom FoeBuD e.V. erinnerte vor der Paulskirche an die Ursprünge der Demokratie, die heute von immer mehr Angriffen auf die Privatsphäre von Bürgerinnen und Bürgern ausgehebelt wird.

Im Anschluss an die Demonstration kündigten die Veranstalter weitere Aktionen gegen die zunehmende Überwachung an. So ist eine Sammelklage gegen die drohende Zwangsprotokollierung von Telefon- und Internet-Kommunikationsdaten in Vorbereitung.

Mehr Bilder und Informationen finden sich unter wiki.stoppt-die-vorratsdatenspeicherung.de/?title=070414-Frankurt-Demo.

Kampagne »SPD, CDU und CSU gegen Vorratsdatenspeicherung« gestartet

Pressemitteilung des Arbeitskreises Vorratsdatenspeicherung vom 18. 04.2007

Der heute vom Kabinett beschlossene Gesetzentwurf zur Vorratsdatenspeicherung stößt auf wachsenden Widerstand in der Großen Koalition. Mitglieder, Mandatsträger und Untergliederungen von SPD, CDU und CSU sprechen sich öffentlich gegen die »drohende Zwangsspeicherung des Telekommunikationsverhaltens der gesamten Bevölkerung« aus. Der Virtuelle Ortsverein der SPD (VOV) unterstützt bereits eine entsprechenden Kampagne des Arbeitskreises Vorratsdatenspeicherung.

Der Appell mit dem Titel »Risiken der Vorratsdatenspeicherung ernstnehmen – und keine Fakten schaffen!« führt Zweifel an der Angemessenheit einer generellen Datenspeicherung und das Missverhältnis zwischen Aufwand und möglichem Ergebnis der Vorratsdatenspeicherung an. »Noch 2005 ist eine generelle, verdachtsunabhängige Speicherung von Verkehrsdaten im Bundestag auf parteiübergreifende Ablehnung gestoßen. SPD und Union müssen zu diesem Konsens und auf den Boden unseres Grundgesetzes zurückkehren«, fordert Patrick Breyer vom Arbeitskreis Vorratsdatenspeicherung, einem bundesweiten Zusammenschluss von Bürgerrechtlern, Datenschützern und Internet-Nutzern.

Erster Unterstützer des Appells ist der Virtuelle Ortsverein der SPD (VOV). Arne Brand, Pressesprecher des VOV, erklärt: »Eine Denkpause ist dringend notwendig, denn es geht um die Wahrung der Grundrechte aller Bürgerinnen und Bürger. Ob mit der Vorratsdatenspeicherung tatsächlich mehr Sicherheit erreicht wird, ist umstritten. Es kann nicht angehen, dass nur das Bundesverfassungsgericht immer wieder die Versuche unverhältnismäßiger staatlicher Überwachung stoppt und per Urteil die Freiheitsrechte wahrt - das zu tun ist zuallererst die Aufgabe der gewählten Volksvertreter.«

Der Appell im Wortlaut:

Risiken der Vorratsdatenspeicherung ernst nehmen - keine Fakten schaffen!

Der Gesetzentwurf zur Neuregelung der Telekommunikationsüberwachung sieht vor, die verdachtsunabhängige und flächendeckende Protokollierung aller Verbindungsdaten der Kommunikation sämtlicher Bürgerinnen und Bürger in Deutschland einzuführen – egal ob per Telefon, Handy, E-Mail oder Internet. Wir, besorgte Mitglieder, Mandatsträger und Gliederungen der Volksparteien SPD, CDU und CSU, fordern die Bundesregierung und die Abgeordneten des Deutschen Bundestags auf, dieses Vorhaben so lange zurückzustellen, bis eine Klärung der berechtigten Zweifel an der Angemessenheit dieses tiefgreifenden Eingriffs herbeigeführt wurde.

1. Zweifel an der Angemessenheit

Die Speicherung aller Verbindungsdaten der Kommunikation völlig unbescholtener Bürgerinnen und Bürger stellt einen schweren Eingriff in das Telekommunikationsgeheimnis und das Recht auf informationelle Selbstbestimmung dar. Wer wann mit wem von welchem Ort aus kommuniziert hat -- dies zu wissen berührt den Kernbereich privater Lebensumstände sowie Geschäftsgeheimnisse. Es ist bisher in keiner Weise überzeugend dargelegt, dass die Speicherung solch sensibler Daten in Fällen, in denen nicht einmal ein Anfangsverdacht vorliegt, angemessen ist.

2. Gefahr des Missbrauchs

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit hat öffentlich vor einem möglichen Missbrauch der Daten gewarnt, die bei zahlreichen Telekommunikationsunternehmen und Internetprovidern gespeichert werden sollen. Schon die Befürchtung von Missbrauch schreckt von unbefangener Telekommunikation ab, auf die Menschen in Notlagen (z.B. bei Gesundheits-, Eheoder Drogenproblemen) ebenso angewiesen sind wie die demokratische Gesellschaft insgesamt (z.B. Schutz von Informanten der Presse als Voraussetzung der Aufdeckung öffentlicher Missstände).

3. Kosten-Nutzen-Analyse

Die Vorratsdatenspeicherung verursacht nach Angaben der Wirtschaftsverbände erhebliche Kosten für die Anschaffung und den Betrieb der notwendigen Technik. Diese Kosten gehen letztlich zu Lasten der Verbraucher und der Steuerzahler und stehen damit beispielsweise nicht mehr für gezielte Projekte zur Kriminalprävention zur Verfügung. Bisherige Möglichkeiten der Telekommunikationsüberwachung und die Möglichkeit, in Verdachtsfällen auf kurzzeitig gespeicherte Verbindungsdaten (bspw. »Quickfreeze«) zurück zu greifen, haben sich in der Praxis als ausreichend erwiesen. Das Missverhältnis zwischen Aufwand und möglichem Ergebnis ist augenfällig.

4. Zweifel an der Pflicht zur Umsetzung der EU-Richtlinie zur Vorratsdatenspeicherung

Namhafte Experten weisen darauf hin, dass für die EU-Richtlinie, die mit dem Gesetz zur Telekommunikationsüberwachung umgesetzt werden soll, keine Ermächtigungsgrundlage besteht. Die Zusammenarbeit im Bereich Justiz und Inneres muss über die »Dritte Säule« erfolgen, in der nur einstimmige Entscheidungen getroffen werden können. Irland hat deswegen eine Klage vor dem Europäischen Gerichtshof angestrengt mit dem Ziel, die Richtlinie für unwirksam erklären zu lassen. Eine vorherige Umsetzung wäre vorauseilender Gehorsam, der uns unter Umständen teuer zu stehen kommen könnte. Diese Klage sollte zumindest abgewartet werden. Außerdem verstößt die Richtlinie nach Meinung namhafter Experten gegen die im Europarecht verankerten Grundrechte.

Wir fordern unsere Parteien daher auf, die Umsetzung der allgemeinen Vorratsspeicherung von Kommunikationsdaten auszusetzen und zunächst in einem offenen Dialog mit ihren Mitgliedern und den Bürgern die Risiken der Vorratsdatenspeicherung zu erörtern. So sehr wir uns eine wirksamere Bekämpfung des Terrorismus wünschen, so wenig möchten wir durch unüberlegtes Handeln neue Gefahren heraufbeschwören und die freiheitlichen Grundrechte einschränken, deren Verteidigung gerade das Ziel des Kampfes gegen Terrorismus und andere Feinde einer demokratischen und offenen Gesellschaft ist!

Appell unterzeichnen:
spdcducsu.vorratsdatenspeicherung.de

Ansprechpartner für Presseanfragen:

- Patrick Breyer 0170-5190598
- Ralf Bendrath, Netzwerk Neue Medien e.V., Bremen: 0179-2154614
- padeluun, FoeBuD e.V., Bielefeld: +49-521-175254
- Werner Hülsmann, FIfF e.V., Konstanz: +49-7531-3659056 oder +49-177-2828681
- Stefan Hermes, Frankfurt: +49-172-6918886
- Ricardo Cristof Remmert-Fontes, Berlin: +49-700-25808789



Bild: Sabine Steinort

Auch BKA-Präsident Jörg Ziercke verwendet eine RFID-Schutzhülle.

In der Anhörung des Innenausschusses des Deutschen Bundestages zur Novellierung des Passgesetzes (Einführung des aufgerüsteten ePasses mit digitalen Fingerabdrücken in RFID-Chip) hat sich auch BKA-Präsident Ziercke als Nutzer einer Schutzhülle für seinen Reisepass geoutet. Während der Diskussion der Sicherheitsrisiken, die von einem unbemerkten kontaktlosen Auslesen des ePasses ausgehen können, zeigte der BKA-Präsident den Ausschussmitgliedern seine Schutzhülle, ohne allerdings etwas zur technischen Ausstattung oder zur Bezugsquelle zu sagen. Ob es sich um ein Eigenprodukt der BKA-Forschung handelt, muss daher bisher offen bleiben. Ziercke vertrat trotzdem die Ansicht, dass von dem ePass für die Bürgerinnen und Bürger keine Risiken ausgingen.